(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11586 A1

(51) International Patent Classification[7]: G08B 29/00

(21) International Application Number: PCT/US00/07775

(22) International Filing Date: 23 March 2000 (23.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/147,321 5 August 1999 (05.08.1999) US
60/152,535 3 September 1999 (03.09.1999) US

(71) Applicant *(for all designated States except US)*: PRINCETON PROTECH LLC [US/US]; 173 Rolling Hill Road, Skillman, NJ 08558 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: KRANZLER, Myles, M. [US/US]; 173 Rolling Hill Road, Skillman, NJ 08558 (US).

(74) Agent: WOODBRIDGE, Richard, C.; Woodbridge & Associates, P.C., P.O. Box 592, Princeton, NJ 08542-0592 (US).

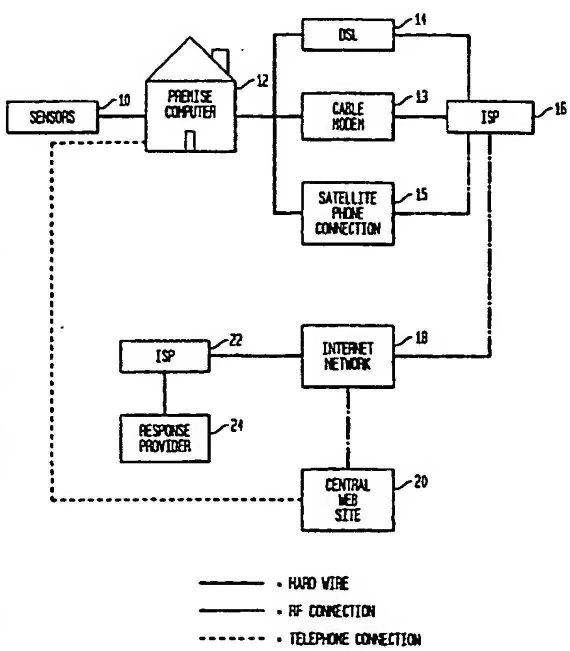
(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ALARM REPORTING SYSTEM USING THE INTERNET AND INSTANT MESSAGING



(57) Abstract: The present invention makes use of the Internet (18) and its instant messaging capability for the continual alarm monitoring of protected premises. A central web site (20) receives instant messages from premise computers (12) at computer controlled, programmable, variable time frames based on protection levels. The protected premise computer (12) sends encrypted messages both in an alarm state and in a normal state. This continual message traffic, reinforced by variable message timing established by the central web site (20) and known only to the central web site (20) and the premise computer (12), provides maximum protection against compromise of the system since the absence of a normal message or the non-appearance of an expected message will constitute an alarm. The central web site (20) dispenses alarm notification to local responders (police, fire dept., local monitors) (24) in accordance with a priority system where the most serious alarm is reported first as well as notifying the premise owners (41) via paging or other communication means. The central web site (20) communicates to the premise computer (12) to change message rates and encryption information as well as to arm the system.

WO 01/11586 A1

TITLE: ALARM REPORTING SYSTEM USING THE THE INTERNET AND INSTANT MESSAGING

CROSS REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the priority of US Provisional Application filed on August 5, 1999 entitled " Monitoring Residential or Commercial Premises Through the Internet" whose inventor is Myles Kranzler and US Provisional Application Serial No. 60/152,535 filed on September 3, 1999 and entitled " Alarm Reporting System Using the Internet and Instant Messaging:" whose inventor is also Myles Kranzler.

BACKGROUND OF THE INVENTION

1. Field of Invention

This invention relates to a means to monitor many premises simultaneously using two way communications via the Internet instant messaging method and a central web site wherein each premise system will communicate periodically with the central web site based on central web site modifiable control parameters.

2. Description of Related Art

The majority of present systems use land line telephone or cellular phones to report alarms to a designated agency. In the normal mode of operation the premise monitoring system locally monitors the status of the alarms and only in the case of a problem seizes the phone line and calls the monitoring agency for help.

This type of telephone system is known to be susceptible to easy compromise. If the phone line is cut or the cellular transmissions are disrupted, the monitoring agency will not know that an alarm is present. The majority of current systems are one way (i.e. from premise to monitoring agency). This makes modification of operation complex. Once a system is programmed for a monitoring site, a change in that site would require a premise visit. This makes it difficult for the monitored premise to change monitors or have a secondary monitoring site in case of emergency at the primary monitoring site.

Current systems are able to use preprogrammed alarm sequences to assist in the determination of whether or not an alarm is false or not. These systems, however, are limited to one way communication and cannot disable or activate selected sensors to accommodate changing conditions or to establish alarm validity. U.S. 5,892,690 issued to Boatman et al describes an environmental monitoring system which includes monitoring assemblies at various sites of environmental concern. Sensors measure environmental parameters, such as air quality and store the data for each site as instructed by an on-site controller . The stored data is uploaded to a central, remote database where it can be accessed and sent out to a particular site. The remote database can be connected to a distributed wide area network, e.g. the Internet. This environmental monitoring system does not include means or procedures for notifying an emergency response agency when a site sensor detects a security breach. This system does not disclose means or procedures for testing the site-to-central database link for failure. The system does not require real time transmission of its data as would be required in an alarm system.

US Patent 5,400,246 issued to Wilson et al describes a peripheral data acquisition, monitor and adaptive control system using a personal computer to allow the user to create a control configuration, test and change and operate the control configuration for diverse applications such as security systems. Measurement and configuration data are entered directly into the computer. Wilson et al discloses such a system adapted as a radio frequency security system for an automobile dealer in which security sensor transmitters are placed in each vehicle and send signals to a central station. The transmissions are logged on the personal computer which takes appropriate action in response, such as, dialing telephones and playing recorded messages to police. Thus the Wilson et al patent also does not suggest an Internet accessible central database to be polled at the convenience of the security agency in accordance with the present invention.

US Patent No.4,741,022 issued to Chebra, et al describes a remote subscriber interaction system. A central control unit (scanner) is connected across a set of subscriber loops. At each subscriber's premises, an individual subscriber terminal (STU) is connected across that particular subscriber's loop. To each STU are connected the various instrumentalities which are to be monitored by the system, e.g. burglar alarms, fire alarms, etc. FSK modulated signals in the upper part of the audible range are transmitted from the scanner to the STUs at appropriate times. The STU's reply by means of similar signals to indicate the status (e.g. alarm, or non-alarm) of the

instrumentalities at the respective subscriber's premises. This transmission and retransmission is interrupted when the subscriber's telephone is off hook. In addition, a signal below the audible range (low tone) is produced at the STU , and transmitted to the scanner over the telephone loop when all the instrumentalities at the particular subscriber's premises are in a given state (e.g. no alarm). When the state of one instrumentality changes, low tone is stopped. Such stoppage is sensed by the scanner, and causes immediate transmission of FSK signals from the scanner to the corresponding STU, even though the associated telephone is off hook at the time. The reply to such transmission provides information about the reason for the stoppage, i.e. what is the source of the alarm.

The Chebra et al system can be compromised by the insertion of a bogus low tone external to the premise and a simulated off-hook condition. The system is dependant on the cooperation of the telephone company and the placement of equipment in the telephone company central office and its volume is limited by the bandwidth of the telephone system. The signals are not encrypted and because they are transmitted at a regular rate can be simulated. When low tone is absent, the interrogation signal sent to the premise during the off-hook condition creates an undesirable disturbance to the user of the telephone.

US Patent No.5,861,804 issued to Fansa et al describes a security and surveillance system controlled by a computer wherein sensors monitor for certain alarm conditions which cause signals to be sent to non-data pins of a serial port of a personal computer. The personal computer produces programmed responses to the alarm conditions. This disclosure relies upon the personal computer and proprietary software to alert security response agencies, for example, by cellular telephone and paging methods. Thus it lacks the central database and polling by remote security response agencies of the database via the Internet that is part of the present invention.

US Patent No.4,477,800 issued to O'Brien, US Patent No.4,647,914 issued to Alexander, US Patent No. 5,136,281 issued to Bonaquist and US Patent No. 5,717379 issued to Peters are of possible relevance as representative of the general state of the art.

The aforementioned inventions fail to suggest a means or procedure for using the instant messaging feature of the Internet, afford protection against compromise through an Internet accessible central database which can be programmed to poll periodically or randomly or on the occasion of a predefined event, encrypt the alarm status using a public key system, or

report alarms in accordance with a priority system where the most serious alarm gets reported first.

SUMMARY OF THE INVENTION

Briefly described, the invention comprises a premise computer, a means of connecting to the Internet such as a cable modem, a wide band telephone connection or a satellite connection, a central web site with computer capability, and the instant messaging capability of the Internet.

The present invention provides a high reliability, large-scale, alarm monitoring capability using the instant messaging feature of the world wide computer network known as the Internet, both to prevent compromise and to avoid the delays in alarm transmission inherent in telephone related systems. The use of the Internet provides two way communication for the purpose of modifying premise configurations through computer control at a central web site, a feature unavailable in typical telephone systems. This capability also allows the central web site to analyze and route alarm information to locally associated response sites in a priority system where the most serious alarm is reported first (a feature not available in normal telephone operated systems).

The continual communication at a defined periodicity rate known only to the premise computer and the computer at the central web site insures that any attempt to compromise the system would itself cause an alarm (premise non-responding). This rate can be modified by random messages sent by the central web site computer to prevent any outside determination of inter-message access.

The use of computers in both premise and Central Web Site permits encryption of alarm data and alterations with the keys under supervisory control.

The invention may be more fully understood by reference to the following drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow diagram that illustrates the process of gathering sensor information and the transmission of that information using the Internet instant messaging system according to the preferred embodiment of the invention.

FIG. 2 illustrates a sequence of events that occur when either an alarm is detected or an "I am OK" message periodic time has expired and shows a sequence of events if no message is

received when expected.

FIG. 3 illustrates a manner in which the Central Web Site determines that the premise requires a modification to its programmed actions.

DETAILED DESCRIPTION OF THE INVENTION

During the course of this description like numbers will be used to identify like elements according to the different views which illustrate the invention. The embodiment described in Fig 1-3 is the preferred embodiment of the system and method of performing the premise monitoring.

FIG 1 illustrates a system 100 for gathering the sensor data and transmitting to and receiving information from the central web site. The central web site **20** instantly recognizes and processes incoming messages through its continuous connection to the Internet **18.** The central web site **20** uses the Internet **18** to transmit messages back to the designated premise containing the sensors **10** through an Internet Service Provider ("ISP") **16.** The ISP **16** is connected to one of three known possible premise communication devices, either a cable modem **13**, a wireless device operating through a satellite **15**, or a wide bandwidth communication system such as a DSL **14**, any one of which permits continuous connection to the Internet. The premise communication devices **13, 14** or **15** are connected to an in-premise computer **12** containing logic control. This in-premise computer **12** receives local sensor data **10** and processes this data in accordance with programmed instructions contained within its logic section.

In accordance with the invention, the premise computer **12** and central web site are initialized on installation with default monitoring information including designation of the sensors **10** connection points and communication protocol (See Fig.2 **21**) The premise computer **12** acquires the data and decides whether the information constitutes one or more alarm states. If it determines that an alarm is present, it will format (see description of **FIG 2**) and initiate the instant message.

If the premise computer **12** is unable to communicate using the cable modem or other communication system (**13, 14 or 15**) it can, alternatively, call the central web site on the telephone. The central web site **20** can download the telephone number if it changes. This information download receives an acknowledgement from the premise computer.

If no alarm state is found, the in-premise computer **12** determines if a periodic "I am OK" message is to be sent and, if so, it. determines if this message is to include raw sensor data.

It then formats the message and initiates the instant message. The decision to send the message containing the raw sensor data is determined by a programmable occurrence counter.

If an alarm state is detected the central web site **20** conveys this information to the selected response provider **24** through the ISP **22** serving the response provider. The central web site **20** receives messages from many in-premise computers and informs the response provider **24** against a priority list where the most serious alarm receives top priority and is reported first (e.g. Should a panic alarm indicate an intruder, such an alarm will receive priority over a report of an open window etc.)

The premise computer **12** receives instant messages from the central web site **20** and updates its control data accordingly. If it receives a "please send last message not received" message from the central web site **20** it re-formats the previous message and re-sends it.

The premise computer **12** can either be a separate device or can operate as a background task on an existing computer.

Referring to Fig. 2, the sequence of events and the central web site **20** processing is described. The premise computer and central web site are initialized on installation with designation of sensor points and communication protocol. The in-premise computer **12** acquires data from all the sensors on a continual basis transmitting such messages to the central web site in a modifiable sequence known only to the premise computer and the central web site and, when the transmission time occurs sends an "I am OK" message or if a sensor changes state, will format **24** the sensor data into a defined packet. The packet is then encrypted **26** using a public key encryption procedure. The private and public keys will be updated at a controller programmed time period by the central web site **20**. The premise computer **12** will have received the assigned central web site **20** public key at a previous time. It includes the central web site **20** public key with each message to permit the central web site **20** to verify the key that was sent. If the in-premise computer **12** loses the key it includes a blank central web site **20** public key to indicate this fact. The encrypted message is sent **28**, using either the cable modem, wireless device operating through a satellite or other wide bandwidth device continually connected to the world wide computer network as an instant message with the central web site **20** (whose address has been programmed into the in-premise computer **12**) as the routing recipient.

The central web site **20** receives the message **30** and using the public key supplied with the message and its own private key, deciphers the incoming message. The central web site **20**

verifies that the message **30** arrived at the expected time and resets the expected time to establish when the next message should occur in accordance with a modifiable sequence. If the message contains sensor change information, the central web site **20** recognizes the status of all sensors and determines **32** if the change in sensor(s) constitutes an alarm or an expected change (e.g. store opening in the morning at 8 am is expected) and if the alarm is true or false based on a predetermined set of scenarios for each premise computer. If a alarm is determined **32,** the central web site **20** determines the designated respondent **24** to that specific sensor **10** and , if a true alarm is determined, forwards the alarm information **36** in accordance with a priority system via the Internet using instant messaging or using telephone numbers previously programmed into the central web site to said respondent **24.** Additionally, if requested, the premise owner is notified **41** by the central web site .The premise computer **12** continues to send the sensor change message at a 'change in sensor designated time frame' until the central web site **20** acknowledges **40** the sensor change message. This acknowledgement is not sent until the local respondent **24** acknowledges the receipt of the alarm message. Once the central web site **20** receives the local respondent's **24** acknowledgement **38,** it sends the premise computer **12** an acknowledgement **40.** The in-premise computer **12** reverts to the standard message time frame. Any change in local sensors recognized by the premise computer **12** are latched (i.e. kept in the changed state internally in the premise computer **12)** until acknowledged by the central web site **20.** Once acknowledged, the premise computer **12** interrogates the sensors active state and, if it has changed back to its original state, the premise computer **12** again reports a change of state. This insures that even a momentary change of sensor state is reported.

If the message contains updated sensor information (not a change) the Central Web Site **20** verifies **30** that that information is consistent with the present stored sensor information. If present stored sensor information is not consistent with the message as received, the central web site **20** responds by initiating a request (see Fig.3, **46**) for additional information including requesting a special response code stored in the premise computer **12.** If this requested information is not returned within a designated period of time or is returned with incorrect data, the Central Web Site **10** notifies (See Fig. 3, **48**) a designated local respondent **24** and, if required, the premise owner **41.**

Every time a message **30** is received from a specific premise computer **12,** of which there is one for every subscriber, the central web site **20** updates the expected time of the next message

30. The central web site **20** has a queue of expected messages and their times. If a message is not received within the expected time (plus a defined tolerance), the central web site **20** initiates and alarm state and immediately notifies **34** the associated respondent **24** and the premise owner **41** .

If the central web site **20** determines that all or part of the means for Internet transmission is disabled, it reverts to monitoring a telephone input for alarm information. If the premise computer **12** does not receive an acknowledgement of its change of sensor message or recognizes that the means for Internet access is down and has a change of sensor, it uses a backup telephone or cell phone to communicate with Central Web Site **20**. This communication method is self limited to reporting only on change of state in order not to overload the telephone system.

Referring to Fig. 3, the central web site **20** can issue requests for sensor data transmission or the retransmission of non-received data to determine loss of communication or verification of premise status. If **46** present stored information is not consistent with a message as received, the central web site **20** initiates a request for additional information including special response code stored in the premise computer. The central web site **20** formats and encrypts **48** the message and transmits to the premise computer **12** using its instant messaging capability. The premise computer **12** decrypts the message and responds **50** to the central web site **20.** If the requested information is not returned **52** within designated period or is returned with incorrect data, the central web site **20** notifies the designated local respondent **24**. Additionally, the central web site **20** notifies the premise computer **12** of changes to reporting schedules or central web site **20** Internet address or backup dial out telephone numbers. Once the transmission request is formatted for transfer to the premise, **53** the central web site **20** sends the message to the premise computer **12.**

The premise computer **12** receives the message **54** and either updates its internal control parameters and / or responds with the requested information.

In summary, the invention provides protection against compromise by transmitting "I am alive" encrypted messages to a central web site monitoring the premise in accordance with a modifiable program known only to that central web site and the monitored premise thereby avoiding bogus "I am alive" messages. The invention makes use of the instant messaging system available only through the Internet to eliminate the delays inherent in standard telephone communication providing the added protection of timely responses to emergencies. The use of the instant messaging system and the two way communication permits the assessment of real or

false alarms in real time and offers the opportunity to eliminate unnecessary police, fire, or medical response.

While the invention herein disclosed has been described by specific embodiments and applications thereof, it is understood that numerous modifications and variations can be made thereto by those of ordinary skill in the art without departing from the spirit and scope of the present invention.

What is claimed is:

1. A system for monitoring premise alarm sensors (10) over a world wide computer network (18).

2. A system according to Claim 1 further comprising that the connection to the world wide computer network (18) shall be from a premise computer (12) through a device including but not limited to a cable modem (13), a wide band telephone system (14), and a satellite connection (15) which is continually connected to the world wide computer network (18).

3. A system according to Claim 2 further comprising means to transmit data from the premise computer (12) to a central web site (20) and from the central web site (20) to the premise computer (12).

4. A system according to Claim 3 further comprising means for the central web site (20) to preprogram the premise computer (12) to issue status messages in accordance with a modifiable sequence.

5. A system according to Claim 4 further comprising means for programming the premise computer (12) with sensor designation and communication protocol with the central web site (20).

6. A system according to Claim 5 further comprising means for programming the central web site (20) to recognize the status of all alarm sensors (10).

7. A system according to Claim 6 wherein the premise computer (12) issues alarm status messages in a modifiable preprogrammed sequence for recognition by the central web site (20) in a matching sequence known only to the premise computer (12) and the central web site (20) such that omission or corruption of the status message represents an alarm condition.

8. A system according to Claim 7 further comprising means where a change in the status of an alarm message initiates a message to the central web site (20).

9. A system according to Claim 8 further comprising a central web site (20) for updating the local premise computer (12) control information.

10. A system according to Claim 9 wherein the data from the premise computer (12) and the central web site (20) is encrypted using a public key methodology.

11. A system according to Claim 10 wherein the status messages can be requested on command from the central web site (20).

12. A system according to Claim 11 further comprising means to use the instant messaging feature of the world wide computer network (18) for requesting immediate reporting of information.

13. A system according to Claim 12 wherein the alarm status is reported to selected response providers (24) and a premise owner (41) in accordance with a priority system where the alarm determined to be the most serious is reported first.

14. A method for monitoring premise alarm sensors (10) using the world wide computer network (18) and two way instant messages wherein said method comprises the following steps irrespective of sequence:

a) programming the premise computer (12) with sensor (10) designation and communication protocol and initiating continual communication with a central web site (20);

b) programming the central web site (20) to recognize the status of all alarm sensors (10);

c) transmitting periodic status messages from the premise computer (12) in accordance with a preprogrammed schedule generated at the central web site (20);

d) indicating a change in the status of an alarm sensor (10) and sending an instant message to the central web site (20) at the time of occurrence;

e) interpreting messages received at the central web site (20) and indicating an alarm status; and,

f) communicating an alarm status to a service provider (24) such as fire, police, or medical facilities in accordance with a priority system.

15. A method according to Claim 14 further comprising the following steps irrespective of sequence:

g) continuously communicating between the premise computer(12) and the central web site (20) using either a cable modem (13), wide band telephone connection (14) or satellite connection (15);

h) activating a public key and a private key in the premise computer (12) and a different public key and private key in the central web site (20)

i) formatting the status of the alarm sensors (10) as a digital message and encrypting the message;

j) transmitting the encrypted message to the central web site (20);

k) decrypting the message at the central web site (20) using its private key;

l) acting upon the message at the central web site (20) in accordance with predefined rules;

m) communicating instructions and commands from the central web site (20) to the premise computer (12) using the premise public key; and,

n) decrypting these commands at the premise computer (12) using its private key.

16. A method according to Claim 14 further comprising the following steps:

o) programming a random code generator at the central web site (20) to periodically establish a timing schedule for premise computer (12) reporting purposes;

p) encrypting and transmitting the schedule to the premise computer (12); and,

q) decrypting the message by the premise computer (12) and adjusting the premise computer (12) clock system to transmit status messages in accordance with the new program.

17. A method according to claim 14 wherein the sequence of alarms reported by the premise computer (12) is used to discriminate between true and false alarms said method comprising the steps of:

r) programming the central web site (20) with the type and location of sensors (10) in the premise; and,

s) transmitting changes from the premise computer (12) as to the status of the alarm sensors (10) and analyzing the changes at the central web site (20) in the status of the alarm sensors (10) against a predetermined set of scenarios to discriminate between true and false alarms.

18. A method according to claim 14 wherein the central web site (20) can update the premise computer (12) control information and said method further comprising the following steps:

t) entering commands into the central web site (20) to change information to the premise computer (20);

u) transmitting said commands from the central web site (20) as priority messages to the premise computer (12);

v) receive and acknowledge the new information at the premise computer (12) and adjust the premise computer's(12) internal control programs to comply with said command.

19. A method according to claim 14, wherein the premise computer (12) will periodically transmit either sensor status or an "I am OK" message using this communication to establish the alarm situation.

20. A method according to claim 14 wherein the reception of a periodic message will itself be considered a no-alarm condition.

21. A method according to claim 14 wherein a central web site (20) can update the local premise computer (12) control information and request immediate reporting of information by using the world wide computer network (18) and instant messages.

22. A method according to claim 14 wherein the central web site (20) transmits alarm data to selected response agencies (24) and the owner (41) using the instant messaging system of the world wide computer system (18) said method further comprising the following steps irrespective of sequence:

w) programming the central web site (20) with the telephone addresses of selected response agencies (24) and the telephone number of the premise owner (41);

x) programming the central web site (20) to report alarms to selected agencies (24) upon receipt of such alarms from premise computers (12);

y) receive from the central web site (20) the status changes indicating an alarm situation; and,

z) connect the central web site (20) to the appropriate agency (24) and report the alarm and telephone the premise owner (41) and report the alarm.

FIG. 1

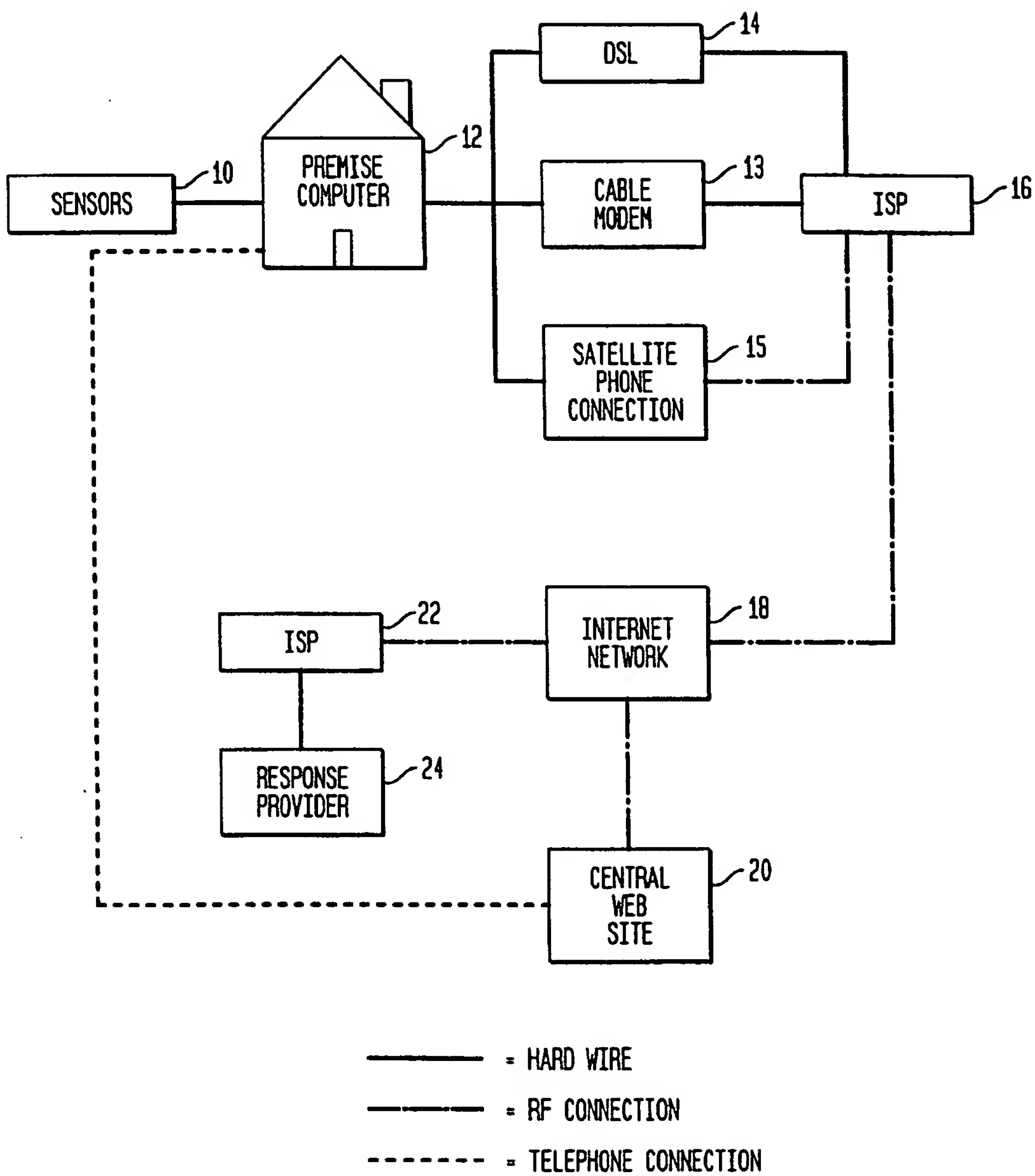

SENSORS
10
PREMISE COMPUTER
12
DSL
14
CABLE MODEM
13
SATELLITE PHONE CONNECTION
15
ISP
16
ISP
22
INTERNET NETWORK
18
RESPONSE PROVIDER
24
CENTRAL WEB SITE
20
= HARD WIRE
= RF CONNECTION
= TELEPHONE CONNECTION

FIG. 2A

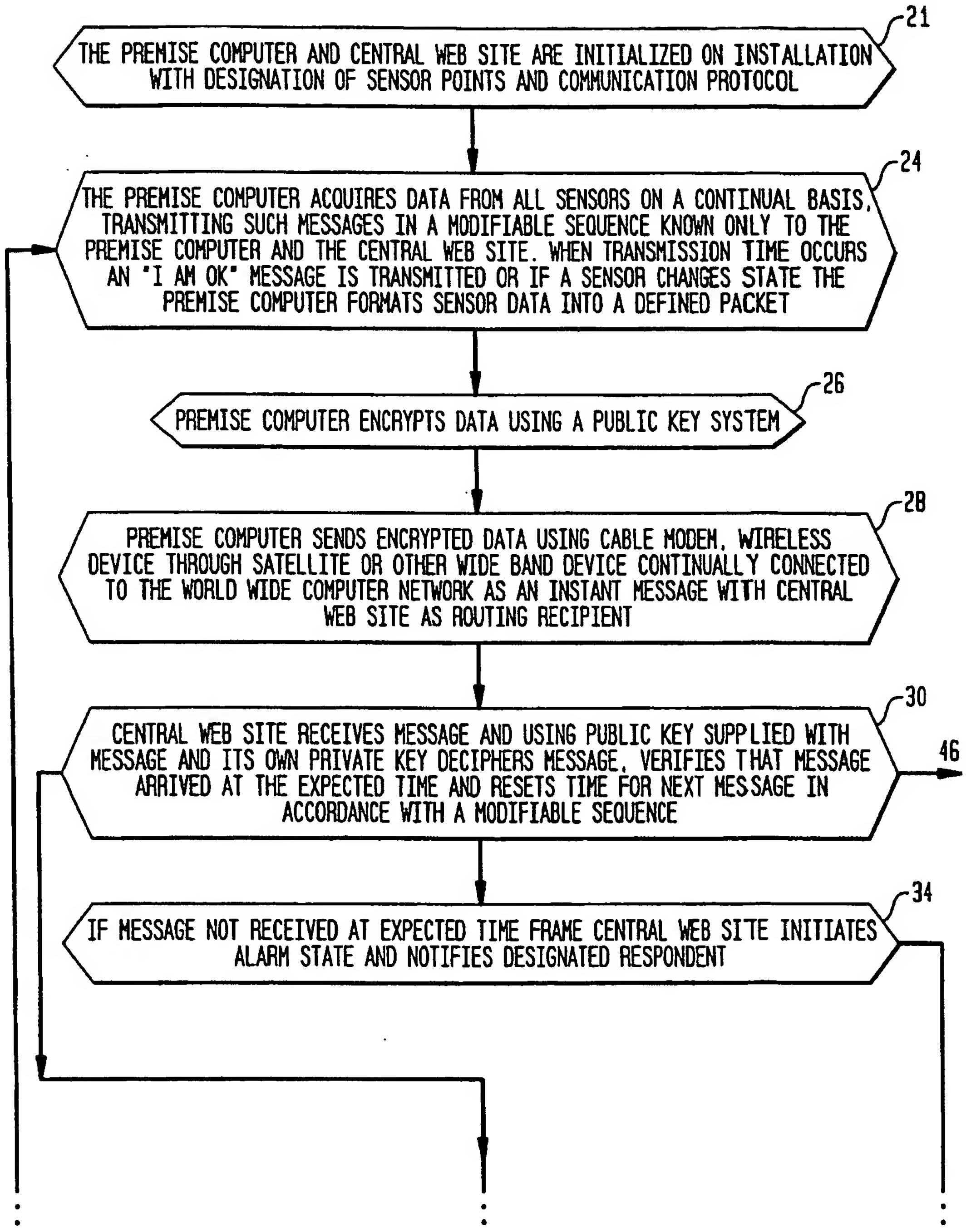

21
THE PREMISE COMPUTER AND CENTRAL WEB SITE ARE INITIALIZED ON INSTALLATION WITH DESIGNATION OF SENSOR POINTS AND COMMUNICATION PROTOCOL
24
THE PREMISE COMPUTER ACQUIRES DATA FROM ALL SENSORS ON A CONTINUAL BASIS, TRANSMITTING SUCH MESSAGES IN A MODIFIABLE SEQUENCE KNOWN ONLY TO THE PREMISE COMPUTER AND THE CENTRAL WEB SITE. WHEN TRANSMISSION TIME OCCURS AN "I AM OK" MESSAGE IS TRANSMITTED OR IF A SENSOR CHANGES STATE THE PREMISE COMPUTER FORMATS SENSOR DATA INTO A DEFINED PACKET
26
PREMISE COMPUTER ENCRYPTS DATA USING A PUBLIC KEY SYSTEM
28
PREMISE COMPUTER SENDS ENCRYPTED DATA USING CABLE MODEM, WIRELESS DEVICE THROUGH SATELLITE OR OTHER WIDE BAND DEVICE CONTINUALLY CONNECTED TO THE WORLD WIDE COMPUTER NETWORK AS AN INSTANT MESSAGE WITH CENTRAL WEB SITE AS ROUTING RECIPIENT
30
CENTRAL WEB SITE RECEIVES MESSAGE AND USING PUBLIC KEY SUPPLIED WITH MESSAGE AND ITS OWN PRIVATE KEY DECIPHERS MESSAGE, VERIFIES THAT MESSAGE ARRIVED AT THE EXPECTED TIME AND RESETS TIME FOR NEXT MESSAGE IN ACCORDANCE WITH A MODIFIABLE SEQUENCE
46
34
IF MESSAGE NOT RECEIVED AT EXPECTED TIME FRAME CENTRAL WEB SITE INITIATES ALARM STATE AND NOTIFIES DESIGNATED RESPONDENT

FIG. 2B

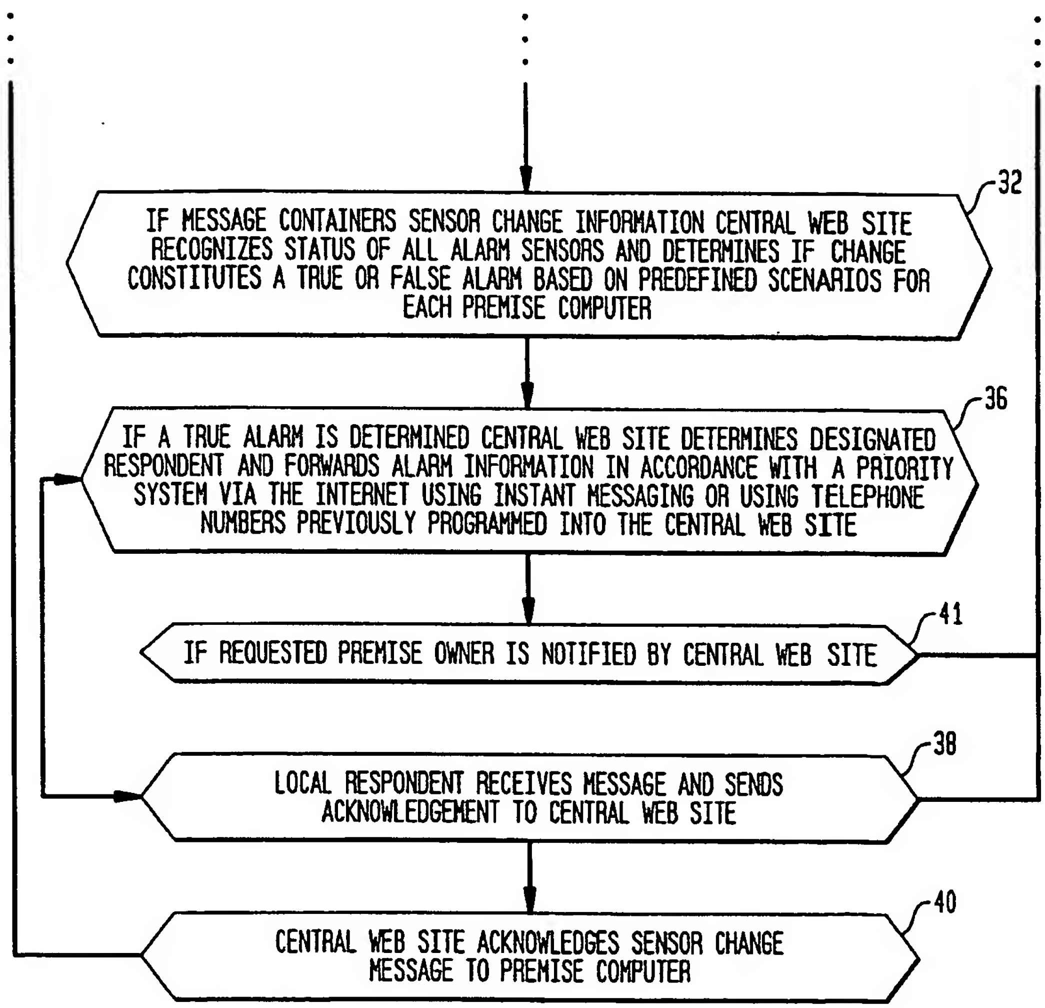
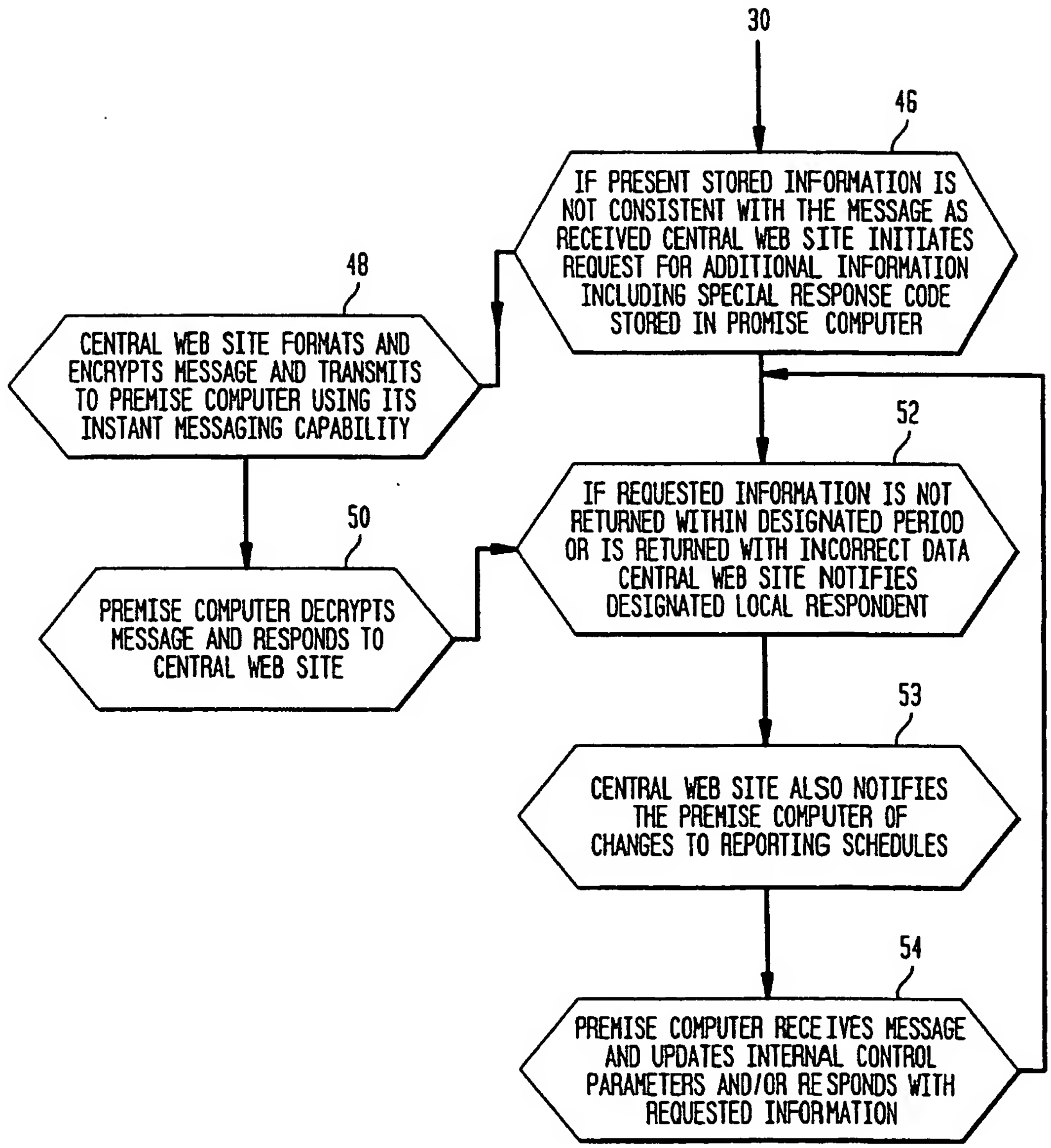

32
IF MESSAGE CONTAINERS SENSOR CHANGE INFORMATION CENTRAL WEB SITE RECOGNIZES STATUS OF ALL ALARM SENSORS AND DETERMINES IF CHANGE CONSTITUTES A TRUE OR FALSE ALARM BASED ON PREDEFINED SCENARIOS FOR EACH PREMISE COMPUTER
36
IF A TRUE ALARM IS DETERMINED CENTRAL WEB SITE DETERMINES DESIGNATED RESPONDENT AND FORWARDS ALARM INFORMATION IN ACCORDANCE WITH A PRIORITY SYSTEM VIA THE INTERNET USING INSTANT MESSAGING OR USING TELEPHONE NUMBERS PREVIOUSLY PROGRAMMED INTO THE CENTRAL WEB SITE
41
IF REQUESTED PREMISE OWNER IS NOTIFIED BY CENTRAL WEB SITE
38
LOCAL RESPONDENT RECEIVES MESSAGE AND SENDS ACKNOWLEDGEMENT TO CENTRAL WEB SITE
40
CENTRAL WEB SITE ACKNOWLEDGES SENSOR CHANGE MESSAGE TO PREMISE COMPUTER

FIG. 3


30
46
IF PRESENT STORED INFORMATION IS NOT CONSISTENT WITH THE MESSAGE AS RECEIVED CENTRAL WEB SITE INITIATES REQUEST FOR ADDITIONAL INFORMATION INCLUDING SPECIAL RESPONSE CODE STORED IN PROMISE COMPUTER
48
CENTRAL WEB SITE FORMATS AND ENCRYPTS MESSAGE AND TRANSMITS TO PREMISE COMPUTER USING ITS INSTANT MESSAGING CAPABILITY
50
PREMISE COMPUTER DECRYPTS MESSAGE AND RESPONDS TO CENTRAL WEB SITE
52
IF REQUESTED INFORMATION IS NOT RETURNED WITHIN DESIGNATED PERIOD OR IS RETURNED WITH INCORRECT DATA CENTRAL WEB SITE NOTIFIES DESIGNATED LOCAL RESPONDENT
53
CENTRAL WEB SITE ALSO NOTIFIES THE PREMISE COMPUTER OF CHANGES TO REPORTING SCHEDULES
54
PREMISE COMPUTER RECEIVES MESSAGE AND UPDATES INTERNAL CONTROL PARAMETERS AND/OR RESPONDS WITH REQUESTED INFORMATION

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/07775

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G08B 29/00
US CL :340/506
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 340/506, 825.06, 521, 539, 531, 825.69; 379/37, 38; 370/913

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
BRS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E --- Y,E	US 6,060,994 A (CHEN) 09 May 2000, col. 2, lines 35-50	1-9 --- 10-17
Y,P	US 5,974,141 A (SAITO) 26 October 1999, Abstract	10-13 and 15-17
Y	US 5,892,690 A (BOATMAN et al) 06 April 1999, col. 1, lines 45-58	14-17
A	US 5,638,448 A (NGUYEN) 10 June 1997, ALL	1-17
A	US 5,917,405 A (JOAO) 29 June 1999, ALL	1-17
A,P	US 6,023,223 A (BAXTER, JR) 08 February 2000, ALL	1-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JUNE 2000	31 JUL 2000

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	JOHN TWEEL, JR. Eugenia Logan Telephone No. (703) 308-7826

Form PCT/ISA/210 (second sheet) (July 1998) ★

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 59-169264

(43)Date of publication of application : 25.09.1984

(51)Int.Cl. H04M 3/42
H04M 3/22
// H04M 3/00
H04N 7/14

(21)Application number : 58-045151

(22)Date of filing : 16.03.1983

(71)Applicant : NEC CORP

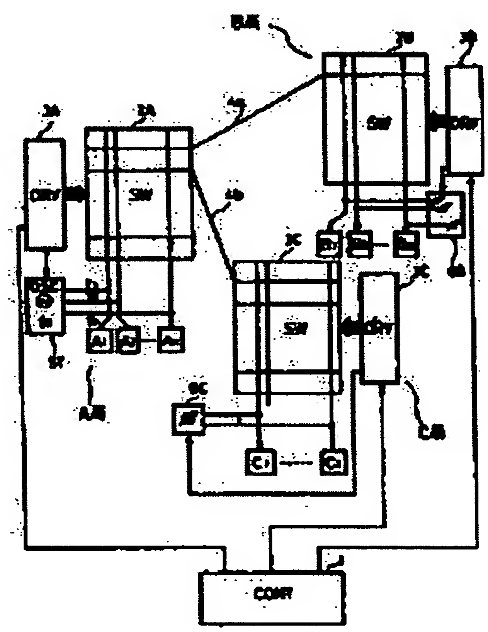
(72)Inventor : YOSHIOKA TAKESHI
SATO TAKAO

(54) CONFIRMING SYSTEM FOR CONNECTION OF LINE

(57)Abstract:

PURPOSE: To confirm a correct connection of a line by identifying the pilot signal having a specific time width which is allotted in response to a subscriber.

CONSTITUTION: For connection between subscribers A1 and B1, a switching command is given to stations A and B respectively from a remote controller 1. At the same time, a command is transferred to the station B to detect the specific pilot signal width T1 of the subscriber A1. Then a switch contact is closed to form a path between subscribers A1 and B1, and the signal T1 is transmitted from the station A. While a correct connection is confirmed at the terminal of the subscriber B1 of the station B as long as the pilot signal received after detection has the time width T1. Otherwise a wrong connection is confirmed if the time width of the received pilot signal is not equal to T1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲ 日本国特許庁（JP）　　⑪ 特許出願公開

⑫ 公開特許公報（A）　　昭59—169264

⑤Int. Cl.³		識別記号	庁内整理番号
H 04 M	3/42		7406—5K
	3/22		Z 7830—5K
//H 04 M	3/00		7406—5K
H 04 N	7/14		7013—5C

④公開 昭和59年（1984）9月25日

発明の数 1
審査請求 未請求

（全 4 頁）

⑤回線接続確認方式

②特　　願　昭58—45151
②出　　願　昭58（1983）3月16日

⑦発 明 者　吉岡毅
東京都港区芝五丁目33番1号日本電気株式会社内

⑦発 明 者　佐藤孝夫
東京都港区芝五丁目33番1号日本電気株式会社内

⑦出 願 人　日本電気株式会社
東京都港区芝5丁目33番1号

④代 理 人　弁理士　井出直孝

明　細　書

1. 発明の名称
回線接続確認方式

2. 特許請求の範囲
(1) 通信回線で相互に結合された複数の交換局の各加入者がこの交換局およびこの通信回線を介して回線接続されたとき、その回線接続を確認する方式において、
各交換局には、
加入者対応に異なる固有の時間幅が割当てられたパイロット信号の発信手段と
各加入者線に到来するパイロット信号の時間幅を識別する手段と
を備え、
回線接続に際して発着信パイロット信号の送出および識別を行い、回線接続の正誤を確認するように構成されたことを特徴とする
回線接続確認方式。

(2) パイロット信号の時間幅は各加入者毎に一定間隔毎に割当てられた特許請求の範囲第(1)項に記載の回線接続確認方式。

3. 発明の詳細な説明
（発明の属する技術分野）
本発明は、通信回線の回線設定による信号パスの接続状態を確認する方式に関する。特にテレコンファレンス（テレビ会議）に適する回線接続の確認方式に関する。
（従来技術の説明）
近年、通信回線サービスは多様化し、従来の電話信号のみならず、データ通信、ファクシミリ等の高度のサービスが行われるようになって来ている。特にテレコンファレンスサービスが注目を集めている。
例えば、テレコンファレンスサービスは、電話に比べて信号の情報量が多いため、テレコンファレンス専用の回線を使用し、また、回線の有効利用を計るためおよび相手先を切替えるためその通

信回線の両端および中間には回線切替スイッチ装置が使用され、加入者の申告あるいは接続要求に対して適時スイッチを切替える。

このようなサービスに固有な専用回線を用いる場合に、電話サービスの場合とは異なり、ダイヤルパルスによって交換機を接続する方式はとらず、センターの制御装置からの指令によって使用する回線の両端および中間の回線切替スイッチを切替える方式がとられる。これは、このような高度のサービスの場合に回線が確実に予約した時刻にサービスできるようにするため、回線の切替えの一元管理するためである。この点が話中状態で接続不能がゆるされる電話サービスとは異なる点である。このような方式では、両端および中間の回線切替スイッチが正しく切替えられ、信号パスが正しく形成されたかを確認することが必要となる。

この確認方法として、従来の方式では、送端から一定の周波数（f_0）のパイロット信号を送り、相手の受端でこのf_0のパイロット信号を受信したか否かを検出することによって信号パスが構成されたことを確認する方式がとられている。

以下第1図によって具体的に述べる。図のA局、B局、C局の3交換局でネットワークが構成されるとし、A局の加入者A_1がB局の加入者B_1とテレコンファレンスサービスを受ける場合に、センターに設置されている遠隔制御装置（CONT装置）1からの指令で、A局とB局のスイッチ切替駆動装置3A、3Bに切替指令が送出され回線切替スイッチ装置2Aおよび2Bのリレー接点が接続され、加入者A_1、加入者B_1の間で信号回線4aを介して回線パスが構成される。次に、パス接続確認のために、加入者A_1よりパイロット信号（一定周波数f_0）をパイロット発振器5より送出し、加入者B_1にて、そのf_0を検出することによって回線パスができたか否かを確認する。

この後に加入者A_1、B_1に対して別に使用可信号（レディ信号）を送り、テレコンファレンスの信号が加入者間に送られる。

しかしこのような方式では同時に、他の回線パス、例えば加入者A_2とB_2間にもパスが構成された場合に、誤って加入者A_2と加入者B_1、加入者A_1と加入者B_2が接続されても、この接続の確認ができない。すなわちこの方法では、例えばA局の加入者A_3の送端からB局の加入者B_3の受端の接続パスと、A局の加入者A_4の送端とB局の加入者B_4の受端の接続パスの構成をチェックする場合に、A局の加入者A_3とB局の加入者B_4が接続されても、全加入者用として同じ周波数f_0のパイロットを使用しているので、A局、B局のそれぞれのスイッチ2A、2Bが動作したことはわかるが、正しく接続されているか否かは確認できず、もし誤接続があれば回線使用者からの申告を待つことになる。

（発明の目的）

本発明は、上記の問題点を解決するものであり、上記のような誤接続を検出できる回線接続確認方式を提供することを目的とする。

（発明の要点）

本発明は、パイロット伝送を含む信号回線と、その信号回線の相手局との接続を切替える回線切替スイッチ装置とで構成される通信回線において、各送信加入者側パイロットにそれぞれ異なる固有の時間幅を割当てるように構成した一定周波数のパイロット発振手段を備え、回線切替スイッチ装置によって接続された相手局側では受信周波数を検出して正しく回線が接続されたか否かを確認する手段を設けることを特徴とする。

特に送信側の固有のパイロット送出時間幅として一定時間間隔毎の信号を割当てることにすれば、パイロット周波数の発生回路が簡略化されるので好都合である。

（実施例による説明）

第2図は本発明の実施例装置のブロック構成図である。遠隔制御装置1の出力はそれぞれスイッチ駆動装置3A、3B、3Cに入力し、上記駆動装置はそれぞれ回線切替スイッチ装置2A、2B、2Cに結合する。交換局A局の加入者A_1～A_nは周波数f_0、時間幅T_1～T_nのパイロット信号を出力する発振器を内蔵しているパイロット発振器5Tに結合するとともに、A局の回線切替ス

イッチ装置2Aに結合する。上記パイロット発振器5Tはスイッチ駆動装置3Aに結合している。B局の加入者B_1～B_mはパイロット検出装置6Bに結合するとともに、回線切替スイッチ装置2Bに結合する。C局の加入者C_1～C_ℓは、スイッチ駆動装置3Cに結合するパイロット検出装置6Cに結合しかつ回線切替スイッチ装置2Cに結合する。パイロット検出装置6Cは到来するパイロット信号の時間幅を識別することができる。

次に第2図の動作について述べる。加入者A_1と加入者B_1を接続する場合に、集中制御装置1よりA局、B局にスイッチ切替指令を、またB局には加入者A_1用の固有のパイロット信号時間幅T_1を検出するための指令が転送され、スイッチの接点が閉じられ、加入者A_1、B_1間のパスが構成される。このとき、A局で加入者A_1の固有パイロット信号T_1が送出される。一方B局では加入者B_1端子ではこの時間幅T_1の信号を検出する。受信されたパイロット信号の時間幅がT_1であれば、これによって、加入者A_1とB_1間の回線パス接続が正しく接続されたことが確認される。

もし、加入者A_2とC_1を上記と同時に切替接続制御し、誤って加入者A_2とB_1のパスが接続構成されると、B局の加入者B_1端子では、加入者A_2の固有時間幅T_2が検出され、すなわちT_1が検出されず誤接続であったことが確認される。

次に、各加入者端子の固有のパイロット送出時間幅として、TからΔTずつ間隔をあけて設定すると、

① パイロット送出時間幅の制御回路は、基準時間ΔTのn倍なので回路が簡単に実現できる。特にT/ΔTが整数の場合と最も簡単である。

② 受信パイロットの時間検出回路は基準時間ΔTまたはΔT/m（m：整数）でサンプリング検出することにより簡単に回路が実現できる。

〔発明の効果〕

以上に述べたように、本発明の方式によれば、それほど複雑な回路を要しないで、接続回線の誤接続の確認をすることができる。話中の許されないサービス、例えばテレコンファレンスシステムに効果がある。なお、テレコンファレンスシステムは一般に双方向回線で行われるが、この場合も上記本発明と同様のことを上り、下り両回線について行うことができる。

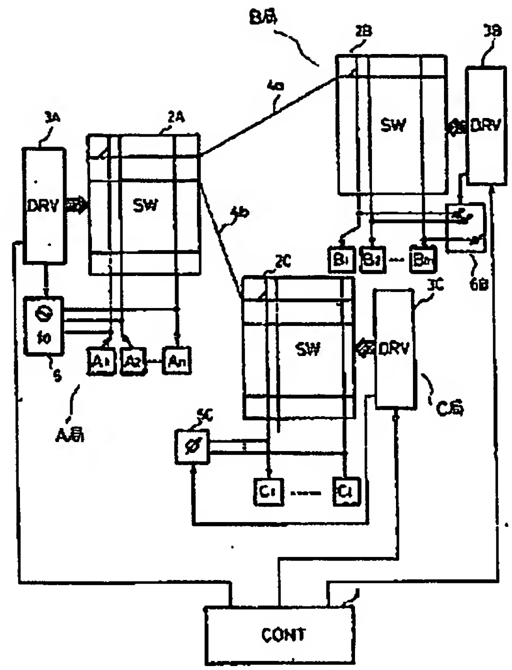
4. 図面の簡単な説明

第1図は従来例装置のブロック構成図。

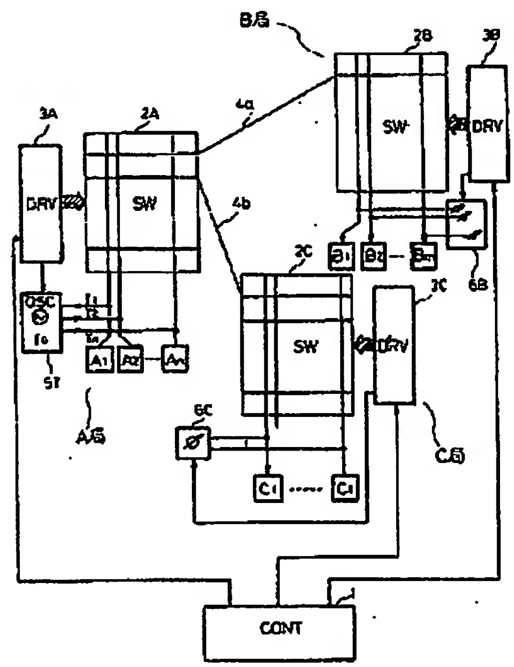
第2図は本発明の実施例装置のブロック構成図。

1…集中制御装置、2A、2B、2C…A局、B局、C局の回線切替スイッチ装置、3A、3B、3C…A局、B局、C局のスイッチ駆動装置、4a、4b…信号回線、5、5T…パイロット発振器、6B、6C…B局、C局のパイロット検出装置、A_1～A_n、B_1～B_m、C_1～C_ℓ…A局、B局、C局の加入者。

特許出願人　日本電気株式会社
代理人　弁理士　井　出　直　孝


B局
2B
3B
4a
3A
2A
SW
DRV
DRV
SW
4b
2C
B1
B2
Bn
6B
3C
f0
5
A1
A2
An
SW
DRV
C局
A局
5C
C1
Cl
CONT

第 1 図


B局
2B
3B
3A
2A
4a
SW
DRV
DRV
SW
4b
2C
B1
B2
Bn
3C
6B
OSC
f0
f1
f2
fn
A1
A2
An
5T
SW
DRV
A局
6C
C1
Cl
C局
CONT

第 2 図

"MP3 Recorder Download - MP3 Recorder - Record Audio Stream to MP3 or WAV," 2002 ttp://www.mp3-recorder.net

MP3 Recorder Download

Record *audio stream to MP3 or WAV* [Bookmark This Site]

MP3 Recorder

Homepage:
Homepage

Download:
Free Trial Download

Buy Now:
Buy Online

Contact:
Contact Us

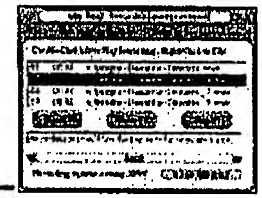
Links:
Exchange Links

Top 3 Downloads
ACE-HIGH MP3 Recorder
Easy MP3 Recorder
Audio MP3/WMA Recorder

Easy MP3 Recorder records any audio source from your computer to MP3 audio directly without temporary WAV files generated. Many useful features inlcude recording list manager, recording time system, recording schedule manager, voice control system, and more ...

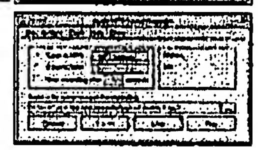
Register It (US$24.95) Download Free Trial

AAA Real Recorder is a sound recording program. It records sound generated, or requested, by other computer programs, such as RealPlayer, Windows Media Player, Quick Time,WinAmp, and many others. The resulting files are saved in wav-file , MP3-file format.



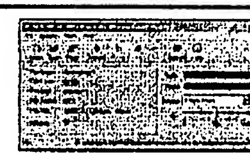
Register It (US$29.95) Download Free Trial

Audio MP3 Sound Recorder offers CD-quality recordings to MP3/WAV. Support recording time length. Recording source is from sound card that means any sound through your sound card would be recorded. Cool skins could be changed to what you like. MP3 VBR is supported with lame encoder for good outputs.



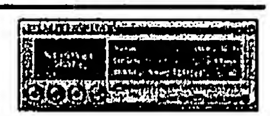
Register It (US$14.95) Download Free Trial

ACE-HIGH MP3 Recorder is professional software designed for recording audio from your computer to hard disk file of MP3 or WAV formats. Comparing with other recording products, our software supports recording to MP3 directly without temporary WAV files generated. With this feature, you may save your hard disk space. And when the ACE-HIGH MP3 Recorder recording, the saved MP3/WAV file's size is calculated and showed on the control panel at real time.



Register It (US$19.95) Download Free Trial

Audio Record Wizard is a sound recorder software, which offers professional recording features with mp3 support.
The audio recorder program is designed to work directly with your sound card, so it can record almost all audio from your sound card at near-perfect quality. So, you can record sound from a microphone, line-in, and just about any other programs (like winamp, realplay, windows media player). audio record wizard can also record

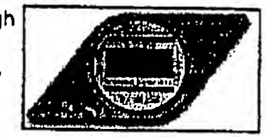


directly to mp3 format if you choose, saving you valuable disk space.

Register It (US$24.95) Download Free Trial

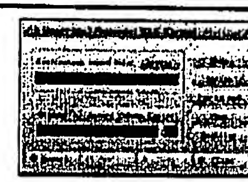
Audio MP3/WMA Recorder makes a complete sound recorder studio of your computer. Sound quality of the recordings remains excellent, or sounds even better for it reduces noise. Audio MP3/WMA Recorder is able to automatically detect the recording formats your sound card supports and then set the application's parameters for the best possible performance. The recordings may be saved as Mp3,Wma or Wav files.

Register It (US$29.95) Download Free Trial



All Sound Recorder enables you to record sound, played back through your sound card and any other sound sources like microphone , VCR, Audio tape player etc. You can use it to grab any sound, including music, dialogs from movies, game sounds etc. from your local computer or the internet. Captured sounds can be saved in WAV or MP3 format, using real-time conversion (without creating temporary files).

Register It (US$19.95) Download Free Trial



Super MP3 Recorder records your computer's audio streaming into MP3 or WAV audio formats. It supports recording sound source from microphone, Internet audio streaming, Winamp, Windows Media Player, Quick Time, Real Player, Flash, Games, etc.

Register It (US$19.95) Download Free Trial

"FAQ Premium Home Answer" eVoice,
http://content.evoice.com/wcs/signUp/FAQ_premHA_s01.htm

eVoice

FAQ

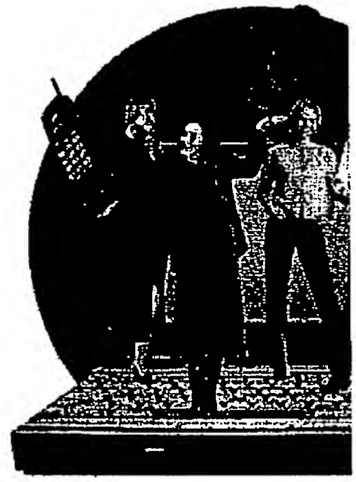
Premium Home Answer

Is It For Me?

FAQ

Demo

Sign Me Up!



What is eVoice?

What does eVoice do?
eVoice is similar to phone company voicemail, but far better. eVoice offers you more f either the phone company or an answering machine. We'll deliver your voicemail direct email inbox and to your home phone. We'll take calls for you when your phone is busy, online and when you're away from home. eVoice will answer after 4-6 rings, or after as as you choose - you decide when you sign up*. When someone leaves you a message, e alert you via email, pager or cell phone. You get free access to your messages from an world via the web at evoice.com. And you can leave a 1-minute personal greeting letti callers know you're not able to answer their call*.

(*=personal greeting and ability to choose number of rings available for eVoice Premiur subscribers only.)

Signing up for eVoice only takes a few minutes at evoice.com.

[B

What else do I get with eVoice?
Check your messages anywhere. With eVoice, you can check your messages by phone,

or have them sent to you as email. Try doing that with an answering machine!

Free long-distance messaging between eVoice subscribers. You can also send voice r other eVoice subscribers anywhere - free. Just call an eVoice access number, enter the number and leave a message. Wherever they are, they can call or check the web to list message. Only eVoice has the features to keep you in touch with the world.

Forward messages from the web: You can forward a voicemail message to anyone wit address. From your eVoice inbox, click the forward button and we'll send the message . RealAudio attachment along with your personal note.

eVoice All Access - combine your wireless phone with your home voicemail: As an e Premium subscriber, you can add a wireless phone to your mailbox for only $2.95 more Now instead of checking voicemail from two places, you can receive all your messages convenient place.

Message broadcasting: eVoice subscribers can send a message to up to 20 subscribers a called QuickDial. It's great if you want to invite people to get-togethers or make an ann Tell everyone with one call!

Phone message management keys: Using any touch-tone phone, you can save, skip, fa rewind, or delete messages at any time. You can even forward them to other eVoice su reply directly to messages sent by other eVoice subscribers without paying long-distanc

[Ba

Where is eVoice available?
eVoice is available throughout most of the US and parts of British Columbia. You can ch messages anywhere on the web or in your email and from practically anywhere using ou numbers. When you start to sign up for eVoice service, you give us the phone number y answer. We'll tell you immediately if eVoice is available in your area. If not, check bac adding service in new areas all the time.

[Ba

Can eVoice answer my wireless phone?
Yes, eVoice customers in several sections of the United States are now able to add a w to their eVoice Premium mailbox, so that one mailbox answers both phones. It's called Access, and we're looking to roll this out to the rest of the US very soon!

Back to Top

"Voice-ASP, White Paper Technology & Processes," eVoice, December 13, 2000

eVoice™

Voice-ASP

White Paper
Technology & Processes

1 Introduction

This White Paper discusses the underlying technology and processes of the eVoice service, focusing on the advantages of eVoice compared to other voicemail and messaging systems. eVoice's ASP-program helps Service Providers (Wireless, Long Distance, CLECs, ISPs, Voice Portals, etc.) deliver next generation enhanced communication services in a reliable and scalable fashion.

2 eVoice Voicemail

eVoice is a nationwide voicemail service that answers home, small office and wireless phones. Calls to the answered phone numbers are forwarded (on Busy or No Answer) to eVoice. If the caller leaves a message, the subscriber is then notified via e-mail and wireless notification and can access the voicemail via phone, the web or e-mail.

3 Service Setup

One of the main ideas behind eVoice's service is to simplify the previously complex call forwarding service setup and provisioning process for the subscriber as much as possible. eVoice streamlines the process by handling all required contact with the subscriber's Local Phone provider. This increases both the sign-up and retention rates.

3.1 RBOC Relationship

eVoice has spent several years developing close relationships with each of the Regional Bell Operating Companies (Bell Atlantic, Bell South, Ameritech, Southwestern Bell, US West and Pacific Bell) and GTE (the term "RBOCs" will be used for this group). The development and maintenance of these relationships allows eVoice to directly accept and process orders from subscribers, eliminating the need for the subscriber to contact the RBOCs directly. eVoice is constantly enhancing its provisioning capabilities (service setup), and additional Carriers (landline and wireless) will continually be added.

3.2 Billing

eVoice's relationships with the RBOCs also include billing arrangements. In most cases, eVoice handles both the set-up and monthly fees that RBOCs typically charge for Call Forwarding. This prevents the addition of fees to the subscriber's RBOC bill, which limits confusion for the subscriber, and reduces customer service calls to the RBOC.

3.3 Order processing

eVoice receives customer orders through both an automated telephone interface and web-based registration forms. These orders are directly forwarded to the correct RBOC using scalable electronic interfaces. eVoice has developed a customized automated interface for each RBOC, to enable timely and efficient processing of

eVoice's large daily order volumes, which currently exceed 2,000 orders per day per RBOC.

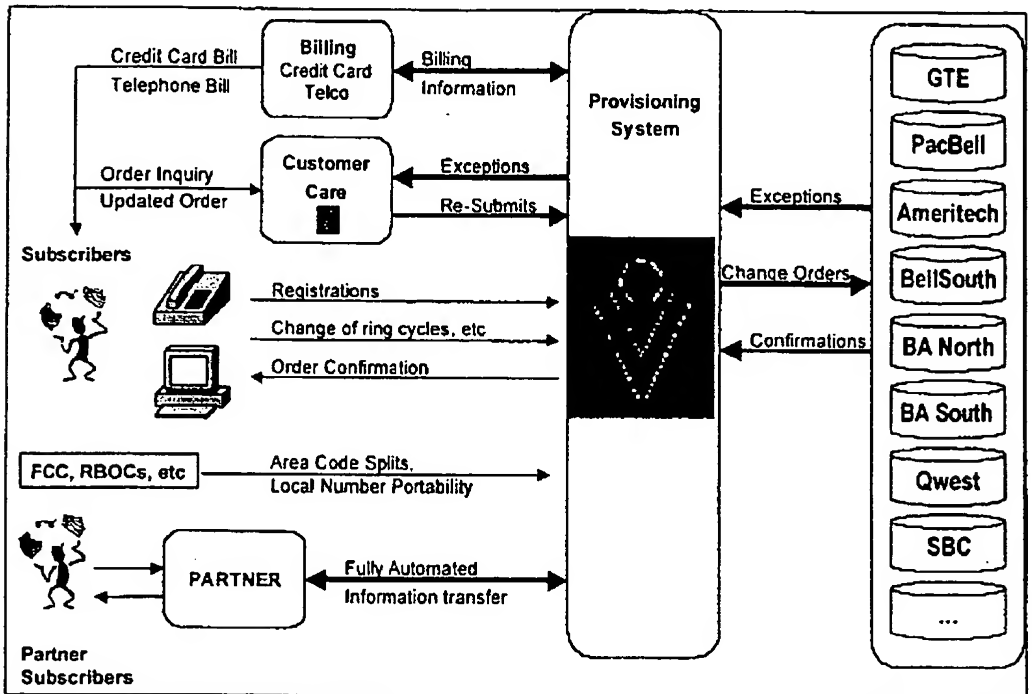


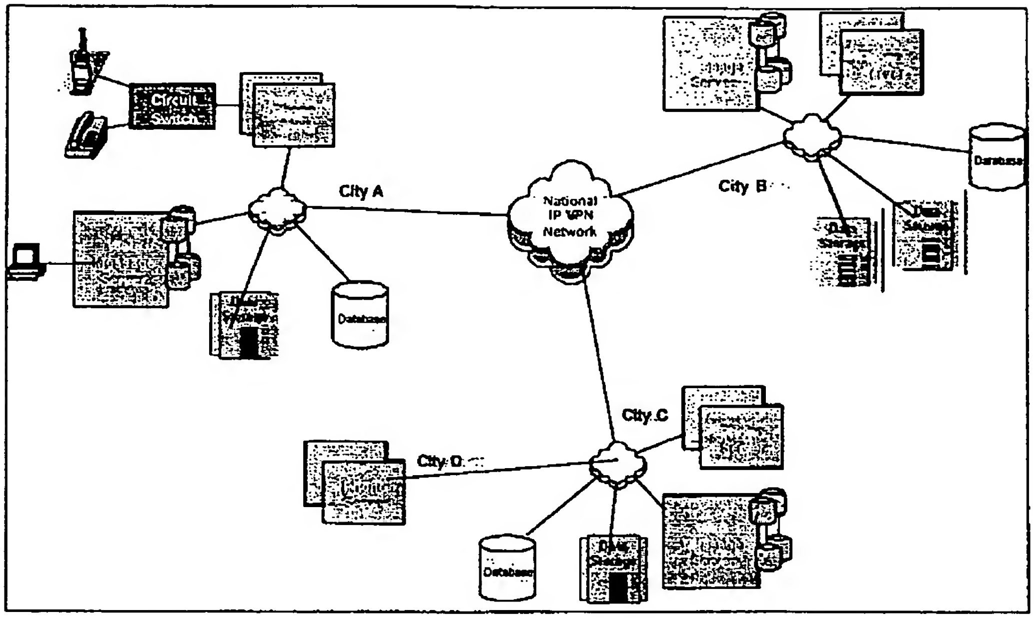
Figure 1 - eVoice Provisioning System

3.4 Exception handling

eVoice has a distinctive, knowledge-based method of handling returned orders, or "exceptions." An RBOC might reject an order or return it for further processing for one of several reasons, e.g.:

- The official number plans provided by the RBOCs are often not fully up-to-date (i.e. do not reflect numbers that have been resold), which may result in an order being sent to the wrong RBOC.
- The customer may have special features enabled on the line that conflict with the new service order.

eVoice has the unique capability to handle these exceptions by simultaneously contacting the customer to resolve the current issue and providing feedback to a rule-based database that is used for order acceptance. eVoice can thereby offer a complete provisioning solution, avoiding the need to train Customer Care staff in RBOC exception handling.



4 Telecom Network

eVoice is the pioneer in deploying IP-enabled voicemail. The path to building out the eVoice network has been much like that of the early ISPs, who had to build their own POPs. Similarly, eVoice has undertaken the process of building and operating an extensive Telecom network. The network has been designed to meet the highest standards of reliability and scalability, while also taking advantage of the low-cost aspects of IP-technology.

Figure 2 – Schematic System Layout

4.1 Local Numbers

eVoice has deployed an extensive Local Number Network, ensuring that every call is always forwarded to a local number. For example, in the San Francisco Bay Area alone, eVoice has over 60 different phone numbers, enabling local coverage of each rate-center (there are often multiple rate-centers within each area-code). All calls forwarded from the called phone number to the voicemail service will be billed by the RBOCs as new calls. Therefore, it is important to have local numbers available, to avoid adding extra costs to the customer's phone bill.

4.2 POP vs. DID

While it is important to provide local coverage for each rate center, this must be balanced with the effort to minimize deployment and equipment cost. eVoice achieves this balance by using POP-technology, enabling eVoice to have exactly one number per rate-center. eVoice uses a Patented software algorithm to identify the incoming call by gathering the signaling from the RBOC, and can thereby open

the correct mailbox automatically. This allows eVoice to minimize the number of forwarding telephone numbers required (each carrying a monthly fee).

Without this sophisticated proprietary technology, competitors must use separate telephone number for each customer (DIDs) in order to identify the correct mailbox. This is an expensive solution, since each number carries a monthly fee. In addition to being expensive, this solution is also not scalable because telephone numbers are a scarce resource, especially in urban areas. Numbers are therefore often obtained in low-density areas, forcing the calls to be forwarded outside the rate-center (and quite often outside the area-code), thereby adding toll-charges to the customer's telephone bill.

4.3 Transport Cost

The POP-network architecture allows eVoice to benefit from the advantages of IP-technology. Message are converted and stored as packages at the closest POP and the message is then transported via IP, if a different POP is used for accessing messages (most messages are left and checked at the same POP, eliminating all need for transport).

Example: A message that is left in San Francisco and is accessed in New York requires only a couple of seconds to transport over IP, whereas conventional (TDM) networks require a managed and monitored long-distance connection for the entire duration (minutes) of the message.

This transport method also eliminates the quality problems that normally plague VoIP connections, which can be expensive to correct and control.

5 System Architecture

5.1 Centralized logic

The eVoice system is built around a centralized and redundant Network Operations Center. This NOC houses all system logic, routing tables, customer profiles, etc. This allows for easy management of the nationwide system, flexible scalability and rapid roll-out of new features.

5.2 Decentralized Data and Message Storage

Messages are stored at the edge of the system, in the POP-servers. This architecture eliminates the potential "single point of failure" problem that is normally associated with a centralized architecture. Each eVoice message is stored redundantly, and the system even recognizes "roaming" customers (calling into the system from different locations) and automatically stores messages at the POP-server closest to the customer.

Customer data is stored in regional and Master databases for both high reliability and fast service. The flexible, decentralized architecture allows eVoice, at the

carrier's request, to store the subscriber data on-site at the carrier's facilities in a mirrored Master database

5.3 Transport

eVoice transports non-real-time messages (IP-packets) between POPs (when needed) instead of streaming voice to a centralized storage place. This transport method is much less costly and more reliable compared to hauling VoIP to a central storage place. VoIP is a good alternative for real-time voice communications, but it has poor economics for messaging and requires extensive maintenance to guarantee the voice quality.

5.4 Mailboxes vs. Phone Numbers

Most voicemail systems are either one-dimensional, where the telephone number is equal to the mailbox ID, or hierarchical, where one telephone number can have several mailboxes (extensions). The eVoice system design allows the best of both worlds by creating separate dimensions for telephone number and mailbox, allowing for a very flexible service setup.

Products that provide voicemail for multiple phones in a single mailbox are now entering the market. This feature will become more popular as an increasing number of people have at least two phones, such as a wireless and a landline. Current solutions often only focus, due to system limitations, on combining business and wireless phones, both phones that are of single user type. The home phone, on the other hand, often has multiple users, and therefore requires extensions, a requirement that currently most systems cannot manage. eVoice's architecture can easily handle this type of configuration, providing both multiple phones and extensions simultaneously, whereas most other voicemail systems only can handle one dimension.

5.5 Notification

eVoice system includes a highly flexible Notification architecture, allowing for notification of subscribers via multiple media. The Notification services are IP-enabled, with the main notification methods being e-mail, SMS and pagers. The subscribers can choose to include a copy of the voicemail in the e-mail, as a Real Audio attachment. The Notification system is already prepared for other media, as Instant Messaging, WAP and Stutter dial-tone, and these methods can swiftly be integrated with the carrier's services.

6 Conclusions

eVoice is well positioned to be the leader in enhanced voice messaging solutions. The unique nationwide home answering capabilities combined with the flexible, reliable and low-cost architecture offer several compelling capabilities for carriers (wireless, IXC, DSL, ISP, CLEC, etc.). The eVoice service can be fully branded and modified to fit the Carrier's current service offerings.

For further information, please contact:

Johan Samuelsson
Director, Voice-ASP
(650) 330 3758
johan.samuelsson@evoice.com

"Voice-ASP, White Paper: Market Opportunities for Enhanced Voicemail," eVoice, November 10, 2000

Voice-ASP

White Paper: Market Opportunities for Enhanced Voicemail

1 Introduction

The enhanced telecommunications services industry is growing rapidly. The convergence of the Internet and telecommunications industries coincides with growing consumer demand for enhanced telecommunications services. This includes services such as call management, call return, caller ID, call completion, call waiting, call forwarding, and voicemail. Voicemail is one of the most valuable enhanced services on the telecommunications landscape today. This is illustrated by recent trends in the residential telecom market where rising prices coincide with increasing penetration, and on the wireless side where voicemail is becoming a required feature for a carrier. This paper discusses the advantages and the value of adding eVoice voicemail (home, small business and wireless) to a carrier's (Wireless, IXC, ISP, CLEC, Voice Portal) current service offering.

2 eVoice Voicemail

eVoice is a nationwide voicemail service that answers home, small office and wireless phones. Calls to the answered phone numbers are forwarded (on Busy and No Answer) to eVoice. If the caller leaves a message, the Subscriber is then notified via e-mail and wireless notification, and can access its voicemail via phone, the web or e-mail. eVoice has developed an automated registration and provisioning process that creates a seamless signup experience for the customer, eliminating all of the hassle associated with contacting the local telephone company.

3 Market Size

The market for these services is growing rapidly. International Data Corporation (IDC) estimates that the consumer voice messaging service market alone will grow from $1.3 billion in 1999 to $2.3 billion in 2003, driven primarily by new subscribers. Current market penetration for voicemail in the U.S. is only 17% and is projected to grow to 30% by 2003, according to IDC. The growth in the number of wireless phone and device users is also driving increased demand for enhanced telecommunications services. Approximately 125 million users in the U.S. subscribed to wireless services in 1999, and this number is expected to increase significantly to 207 million users by 2004, according to IDC. Furthermore, it is believed that enhanced telecommunications services are the most profitable part of most regional phone companies' revenues which also makes this an attractive market segment.

3.1 Challenges for Consumers

As the number of wireless, Internet, and telephone users has increased dramatically in the past few years, the consumer demand for enhanced telecommunications services has outpaced the degree to which these services are streamlined and integrated. Many consumers with more than one phone number currently need to access multiple voice mailboxes to retrieve their messages, which is costly and time consuming. The emergence of wireless phones with visual interfaces such as Wireless Access Protocol (WAP) does not fully address consumer needs. Wireless users, especially while driving, desire more convenient access to communications.

In addition, many consumers accessing the Internet use dial-up connections and have only a single home phone number, meaning they cannot receive incoming calls while they are online. Incoming calls go unanswered or are forwarded to voicemail for many such consumers, and callers typically have no way of knowing if the person they are trying to call is online. This creates a significant consumer need for the type of call control that eVoice provides.

3.2 Challenges for Carriers

Recent deregulation of the telecommunications industry has greatly reduced barriers to entry for telecommunications service providers. The elimination of these barriers has increased competition for Regional Bell Operating Companies (RBOCs) and created opportunities for new entrants such as Competitive Local Exchange Carriers (CLECs) and long distance carriers, also known as Interexchange Carriers (IXCs), to enter regional markets. Deregulation has also enabled relative newcomers such as Internet Service Providers (ISPs) and enhanced telecommunications services providers, such as eVoice, to enter the market.

The rapid changes in the telecommunications industry have created significant challenges for many of these CLECs, IXCs, and ISPs. In response to increased consumer demand for enhanced telecommunications services, many carriers would like to add new features and functionality to their offerings to distinguish their brand, reduce churn and add incremental revenue streams. However, adding incremental enhanced services to a carrier's offerings is both time consuming and costly, requiring the carrier to build new infrastructure, deploy new operations support systems, and develop expertise in Internet and voice web technologies. Its believed that many carriers will find it economically more attractive to purchase enhanced services from an Application Service Provider (ASP) on a wholesale basis and re-brand them as their own, than to develop them internally.

4 The Value of Voicemail

This section discuss the different ways carriers will benefit from adding eVoice voicemail to their current offerings.

4.1 Monthly Fees

RBOCs (Bell Companies + GTE in this paper) are currently offering Home voicemail at a price between $6-10 per month[1]. eVoice Home voicemail offers several enhanced features (Web access, e-mail notification, etc.) that makes it a superior product to the current RBOC offering, and thereby justifies a similar Monthly Fee. Customers prefer monthly fees with unlimited (or close to unlimited) service rather than measured services that charge on a per-message basis. Flat fees are also preferable from the carrier's perspective, because they tend to foster increased usage which enhances the bond between the carrier and the customer.

[1] It is important to add the fees for the separate but required Forwarding feature when looking at RBOC voicemail pricing. These fees are typically not included in the quoted price.

Example	
Monthly voicemail fees (RBOC prices)	$7-10
Set-up fee (RBOC prices)	$10-15

4.2 Increased Usage

The value of increased usage of the main service is most clear for wireless carriers, but Long Distance Companies (IXCs) will also get a boost in usage and thereby revenue. An often quoted example of the benefit of adding voicemail is the "*Zero calls vs. Three calls*" scenario. An unanswered call to a phone without voicemail will result in *Zero* completed calls, whereas by adding voicemail, there will first be a call for leaving the message, a second call for checking the message and finally a third call when the called party calls back the caller. This results in *Three* completed calls, all of them chargeable (although message leaving is usually free of charge). This is the main reason that many new PCS providers and overseas carriers have added voicemail as a Free-of-charge feature to their wireless services.

Adding more minutes of use in today's world of "big bucket" wireless plans is often mistakenly considered to be negative or neutral, under the idea that "there are plenty of minutes left in the bucket and more minutes will not generate any new revenue." This is not true, since there will always be some subscribers that will be "pushed" into the next bigger bucket or pay for minutes over the bucket-limit. Averaging this revenue over all subscribers will show that each added minute will generate revenue. It is also important to driving as much usage as possible from the local phone to the wireless, causing landline migration. The wireless competition will continue to drive larger buckets and lower prices. It is therefore important to fill up these buckets in order to keep the ARPU[2] steady.

Example - Wireless	
10 extra "return" calls per month at 3 min = 30 extra minutes	
Marginal revenue per minute– 15 cents.	
Additional Monthly revenue due to voicemail =	$4.50

4.3 Lower Churn

Controlling churn (customer retention) is today's most important business issue for Telecom carriers. Increasing acquisition costs combined with tighter margins require the carriers to extend the relationship with each customer as long as possible. Lowering the monthly churn for wireless carriers with just 0.1% will increase the lifetime revenue by more than $90[3]. According to IDC, "*the best way to reduce churn is to build a relationship with customers. One way of doing this is to bundle services.*" Adding voicemail is one of today's best bundles, proven by the fact that

[2] *Average Revenue Per User*

[3] *Current average wireless churn is 2.2%. Data from DLJ "Global Wireless Communications Industry" report, Summer, 2000.*

most new PCS providers choose to include voicemail as part of the PCS service bundle at no additional charge to the consumer.Communication with the customer is also an effective churn reduction tool. Most telecom carriers only have bill inserts, or, even worse, a line on a credit card statement as their only communication vehicle. eVoice web-enabled voicemail has proven to be a great communication vehicle, allowing the carriers to communicate with the customers daily in a one-to-one dialogue, via the web in-box.

Home voicemail is an excellent addition to the service bundling because it is not directly associated with the carrier's main product. Cancellations will thereby affect not one but two important services, making it much more difficult for the customer to leave the service.

Example - Wireless	
Lower churn from 2.2% to 2.0% will add to lifetime revenue	$180

4.4 Lower Cost

eVoice voicemail is based on state-of-the art software running on high-capacity IP-based servers. This configuration will dramatically reduce the cost per customer compared with traditional voicemail systems with proprietary hardware and software modules. The outsourced model will also lower management and maintenance cost for carriers, without reducing the carrier's control and reliability. (See also Section 5.2, Pay-per-Feature).

4.5 Differentiation

eVoice's nationwide home answering capability and highly customizable access and notification options provides carriers with an opportunity to differentiate their products from those of competitors. The basic service alone will give carriers an edge, and eVoice's flexible platform allows for extensive integration with carrier's existing products which allows for the ongoing development of new innovative services. Telecom services are rapidly becoming commodities (the ISP-industry is a recent example). Differentiation will allow carriers to avoid the price pressure and remain competitive (AOL being the outstanding example from the ISP-industry).

4.6 Increased Web-traffic

Web access is a great complement to the traditional phone interface for voicemail. The web inbox integrates neatly with the carriers current web-site[4]. This will give a dramatic boost in traffic to the carrier's web-site. Customers will visit the site to check for voicemail several times per week, allowing for promotion of the carrier's other web-services such as e-commerce, e-customer care or up-sell of other products. This will help the carrier to achieve the cost savings that the addition of web-services promised to deliver.

[4] *eVoice will handle the integration.*

4.7 Add-on Sells

eVoice voicemail offers several opportunities for selling additional revenue-generating services. Multiple Phones, Extensions and Internet Call Waiting (ICW) are several of the many features that can be added to eVoice service, generating added revenue per subscriber.

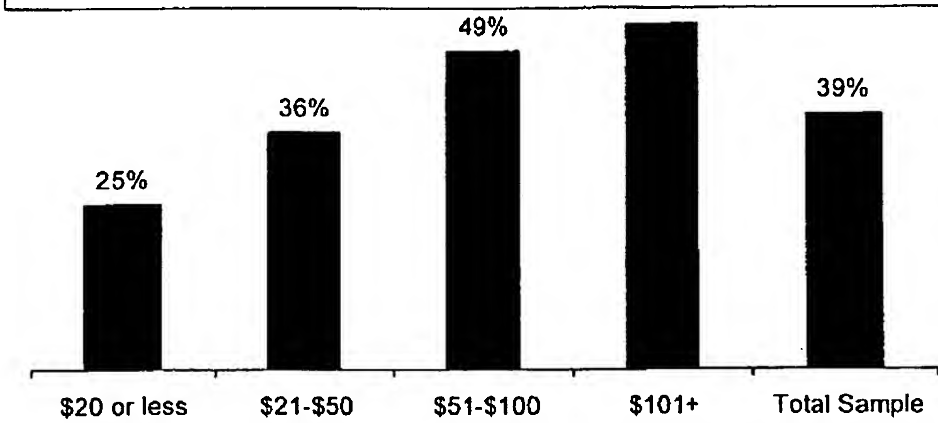
Example	
25% of subscribers with extension at $2.95/extension	$0.75
20% of subscribers with Multiple Phones at $4.50/extra phone	$0.90
20% of subscribers with ICW at $4.95/subscriber	$0.99
Average 20 minutes LD from voicemail platform at 10c	$2.00
Total extra revenue per subscriber	**$4.64**

4.7.1 Multiple Phones

Adding multiple phones into one single mailbox is a frequently required feature by today's busy consumers, that often are forced to check voicemails in multiple places. Several Bell Companies (Bell South, Pacific Bell and US West) have or shortly will launch this type of service. eVoice, with its home-answering capabilities, is the only company that can offer the same service for non-RBOC companies. 39% of wireless users indicate that they are interested in adding home voicemail to their wireless voicemail and 41% state that the availability of this service would influence their choice of wireless carrier[5]. This creates a sizeable market opportunity, and the interest increases among the higher-spending segments of the wireless customer base.

[5] *Market study performed by Insight Express, ordered by eVoice. Contact eVoice for more information.*

Figure 1 - Wireless Subscribers interested in adding Home voicemail to their Wireless service, segmented by monthly wireless spending (ARPU).



4.7.2 Extensions

RBOCs currently charge between $2-4 for each extension that is added onto a home voicemail box. The eVoice product that routes Multiple Phones into a single voice mailbox will require an enhanced usage of extensions for home phones, since home phones are often shared whereas wireless phones are private. 10% of eVoice current users are already using extensions for a single phone, a ratio that is increasing. The increased usage of extensions that comes with the Multiple Phones product makes the extensions feature that eVoice offers even more valuable.

4.7.3 Internet Call Waiting

Internet Call Waiting (ICW) allows customers to receive notification and to answer calls when they are on-line. ICW allows customers to avoid paying for a second phone line while still enjoying many of the benefits, reducing their overall telecom spending. This advantage is also available with the basic eVoice service, but ICW adds enhanced flexibility of how to handle incoming calls. Most ICW services are today in the range of $4-7 per month.

4.8 Platform for other services

The eVoice platform provides carriers with an excellent foundation for adding other telecommunication services . The frequent use of voicemail serves as the entry gateway for less frequently used but highly profitable services as Directory Assistance, Calling Cards, Voice Portals, etc. The flexibility and reliability of the eVoice platform allows for easy integration of other services.

4.9 Example

This example demonstrates the extra revenue that would be generated by adding home voicemail to a wireless carrier's existing product.

Each home voicemail customer will generate revenue in several categories: monthly fees, extra airtime and enhanced features (extensions and ICW).

Monthly Fee	$6.95
Extra Airtime	$4.50
50% penetration of extensions at $2.95	$1.47
20% penetration of ICW at $4.95	$0.99
Total added revenue per home voicemail subscriber	**$13.91**

Reducing churn from 2.2% to 2.0% will add an additional customer lifetime revenue of $180 (or $236 including the new Home voicemail revenue).

The take-rate for home voicemail is assumed to be 20% (using the rule of thumb that 50% of survey respondents that indicated interest will actually sign up for the service). Revenue will increase by $2.78 per subscriber, or by 5%[6] - a significantly increase in carrier's revenue.

5 Advantages with Voice-ASP

The Application Service Provider-model offers many advantages for carriers, and eVoice Voice-ASP brings these advantages for voice-services.

5.1 Time-To-Market

The initial integration of eVoice voicemail will be done in weeks instead of months of planning and installation of dedicated voicemail platforms. Add-on features can be added in days.

5.2 Pay-per-Feature

One of the greatest advantages with ASP is the possibility for the carrier to pay per subscriber and per feature. There is no need to build and pay in advance for capacity that will mostly be unused, or to upgrade the whole platform for enhanced features that only a small percentage of the customer base will use. EVoice offers a pay-as-you-go model where the carriers only pay for the services and feature they actually use.

[6] Based on an average ARPU of $55 for wireless carriers – DLJ's "The Global Wireless Communication Industry" Summer 2000 (Dick Tracey).

6 Value per Category

6.1 *Wireless*

Because the eVoice solution enables wireless providers to combine a user's land line voicemail with wireless voicemail, wireless users with eVoice service will use their wireless phone more often (to access their land line voicemail), resulting in increased minutes of use (MOU). As eVoice extends the capabilities of the platform in communications, content and commerce, this will further drive increases in MOU. These capabilities could provide a significant source of additional revenue and service differentiation and help reduce churn for wireless providers. In addition, the web features should attract users to the wireless carrier's website, providing opportunities for up-selling.

6.2 *Long Distance*

With the continuing deregulation of the telecommunications sector, RBOCs are beginning to provide long distance telephony service and are aggressively pursuing the $40 billion U.S. long distance market. Long distance carriers, also known as Interexchange Carriers (IXCs), resell local phone service, but do not have the right to resell the RBOCs' voicemail service. This inability puts the IXCs at a competitive disadvantage. By partnering with eVoice, IXCs will be able to provide customers with a more complete, competitive telephony solution. Furthermore, eVoice voicemail solution is superior to that of the RBOCs, and that this will enable IXCs to not only reduce churn, but also to increase their monthly billing revenues and their market penetration.

6.3 *CLECs*

Since deregulation in 1984, a large number of CLECs have been formed to compete for local service. CLECs have primarily been providing call completion services, and typically do not derive much revenue from enhanced services. In order to more effectively compete with the RBOCs, CLECs will need to offer more enhanced services, such as voicemail. By offering eVoice voicemail service, not only will CLECs have an additional revenue stream, but they will also have a superior service versus the RBOCs, thus improving customer acquisition and reducing churn.

6.4 *The ISP, Instant Messaging (IM) and Internet Portal Markets*

ISPs and online portals have strong customer bases with high usage, but limited presence in the voice market. Several of the online portals have added "voice chat" capabilities to their instant messaging products and also launched "PC to phone" capabilities. These portals do not typically have access to their consumers' home phones, and therefore, have not offered solutions that generate significant revenue from these home subscribers. eVoice enhanced messaging, IM and Internet Call Waiting capabilities can provide a compelling product for these ISPs and portals which should allow them to bypass the local phone companies. eVoice automated provisioning will allow ISPs to deliver advanced features such as Internet Call Waiting, so that users may manage inbound phone calls while staying connected on their dialup line. Also, web-based inbox provides web portals with an opportunity to

increase stickiness by enabling users to retrieve their voicemail messages and perform other communications functions from their website, every day.

6.5 Voice Portals

Advances in voice recognition technologies are enabling the emergence of "voice portals." A variety of new companies in the enhanced telecommunications services market are providing such useful content; however, companies that enter this market face two primary challenges: customer acquisition costs and telephony network costs. eVoice nationwide network and installed base of customers position address these issues. By integrating voice portals into the network, eVoice can significantly reduce the voice portal's telephony network costs and customer acquisition costs. eVoice can also provide low-cost user acquisition to voice portals by promoting the voice portal to the base of daily voicemail users, offering the convenience of direct-connect to the voice portal from the eVoice platform.

6.6 Summary

The table below summaries the opportunities for Value Creation for each segment.

	Wireless	IXC	CLEC	ISP	Voice Portal
Monthly Fees	★	★	★	👍	☑
Additional service usage	★	👍	☑	☑	☑
Lower Churn	★	★	★	★	★
Lower Cost	👍	👍	👍	👍	★
Differentiation	★	★	★	★	★
Increased web-traffic	👍	👍	👍	★	★
Enhanced features	★	★	★	★	👍
Value Creation:	★ *- Significant*		👍 *- Healthy*		☑ *- Some*

7 On-line Marketing of Voicemail

Voicemail is a traditional telecom product that works well with normal marketing methods. However, the web-based inbox and registration have allowed eVoice to rely heavily on on-line when marketing its own brand of voicemail, with great result. It is therefore recommended to tap into on-line marketing as much as possible when designing marketing plans.

An even more important fact is that online marketing perfectly targets users of web-based voicemail. Once a customer has signed on for eVoice web-based voicemail,

the preferred marketing vehicle for that customer will be on-line, thereby significantly lowering future acquisition cost.

8 Conclusion

eVoice is uniquely positioned to offer carriers new profitable revenue streams, and at the same time lower churn and enhance differentiation. eVoice flexible platform allows for speedy and simple integration with the carriers current services. voicemail is already today one of the most valuable voice-services, and with eVoice, its full capacity is un-leashed.

For further information, please contact:

Johan Samuelsson
Director, Voice-ASP
(650) 330 3758
johan.samuelsson@evoice.com

"Audio Digitizing Process,"
TalkBank,http://www.talkbank.org/da/audiodig.html

TalkBank Audio Digitizing Process

What you will need:

1. Audio source (DAT, casette, minidisk, or reel-to-reel)
2. Power supply for the audio source
3. Mini-mini or RCA-mini audio cable
4. Headphones or speakers
5. Mac or Windows computer
6. Digitizing software:

- For older Macs: Sound Edit 16 (http://www.macromedia.com/software/sound/)
- For Windows: CoolEdit (http://syntrillium.com/). Also, Windows provides sound recording in the System Accessories panel for free, although this feature has some limitations.
- For OS X: Peak 3.0 (http://bias-inc.com). There are also several freeware and shareware recorders, but they have various limitations.

Connecting the output source to the computer:

The first step in digitizing a sound file is to connect the audio source (DAT, casette, minidisk, or reel-to-reel) to the computer. We will refer to the input audio source as a tape recorder. However, DAT, casette, minidisk, and reel-to-reel all work in essentially the same way. Then connection is usually done by connecting a mini audio cable from the headphones output on the tape recorder to the sound input on the computer or sound card. For better sound quality we used to recommend going through the line output and not the headphones. However, newer sound cards make it possible to use the headphone output. If you are able to get a good level of audio input from the headphones jack, you can skip reading the next section.

Using a mixer:

Some combinations of older hardware (often reel-to-reel and sometimes DAT) and older sound cards cannot make good use of the output from the headphones jack. In these cases, you need to use the line output from the audio source. The problem with using the

line output is that you often cannot control output level or volume (although some audio sources have a control for this). If the output level of the line output of your machine does not match that required by the computer, you will overdrive the input and get bad results. Newer sound cards seem to have solved this problem and it is usually possible to use line input for recording.

If this situation arises, you will need to use a device to control line output level. Another reason to have a device to control line output level is that, if the tapes are of poor quality or contain a large range of volume levels you will need to adjust the sound manually at various points in the tape in order to prevent clipping. The best solution is to use a mixer. The Studio Master 42DC which costs $65 can be purchased from Full Compass Audio (800 356-5844). Audio technicians tell us that mixers are better than amplifiers. However, we have not noticed an audible difference. Running the tape recorder through an amplifier allows volume control while maintaining the sound quality.

Setting up your connections in the simplest case

1. Get a mini-mini stereo cable.
2. Plug one end into the headphones output of the taperecorder.
3. Plug the other end into the computer's microphone input jack
4. Plug headphones or speakers for monitoring into the computer's headphones jack.
5. Open up SoundEdit16 of CoolEdit -- you don't have to start recording yet. Just have it open.
6. Start playing the tape and listen to the sound. Observe the sound level and make sure that it does not go into the red zone. This feedback is in the Levels window in SoundEdit. It is less clear in CoolEdit.
7. You can control the sound level with the tape recorder volume controls.

Setting up your connections when you have an amplifer or a mixer

1. If you have a mini output on your taperecorder, you need a mini-dual-RCA cable
2. If you have a dual RCA output on your taperecorder, you need a double RCA cable.
3. Plug the correct end of one of these cables into your tapecorder's line output.
4. Plugs the other end of one of these cables into your mixer or amplifier's line in.
5. Now you need another cable to connection to your computer. This should be a dual RCA to mini cable.
6. Plug the one pair of RCA plugs into the mixer's line output.
7. Plug the mini jack into the computer.
8. Plug your headphones into the computer's headphones jack.

9. Open up Peak, SoundEdit16 or CoolEdit-- you don't have to start recording yet. Just have it open.
10. Start playing the tape and listen to the sound.
11. You can control the sound level with the amplifier or mixer volume controls.

Sound Settings

Sounds settings for your card change with each version of the operating system, so we cannot give instructions that will be valid for all users. Basically, you just have to read your computer manual for this. Make sure that you have the input and output settings adjusted to tape input from the external audio source and to play back to speakers or headphones if you want to monitor the recording.

Using Sound Edit 16 and CoolEdit

We describe the recording process here for SoundEdit 16. CoolEdit and Peak work in much the same way. For CoolEdit, try to ignore the complex interface and just focus on the recording buttons down at the bottom left of the screen. For SoundEdit 16, recording will default to 44,100 Hz, 16 bits, mono, with no compression. This is OK for recording. However, you will probably want to save the file at 22,050.

The Controls window

The Controls window in Sound Edit 16 is used to record sound, play a sound file and stop or pause the recording. You can also use the controls pull down menu at the top of the screen for the same options.

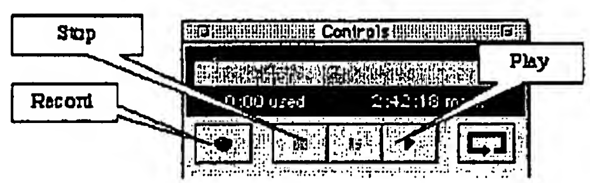


Figure 2: Control Window in Sound edit 16

Monitoring Sound levels

The Levels window allows you to monitor and control the recording and playback levels in Sound Edit 16. For the best results, in the recording window, make sure to set the L/R volume to –16. This setting is recommended by Sound Edit for obtaining the best over all sound quality.

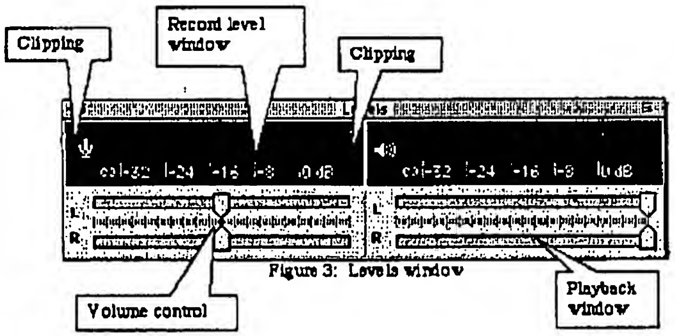


Figure 3: Levels window

If a red dot or red block appears in the recording levels area the sound is being clipped. Clipping is defined by Sound Edit as the amplitude of a sample exceeding the quantization range. For example, if a child is sitting to close to the microphone and starts to scream the top and bottom of the wave form will be cut off. This results in a very poor digitized sample.

In order to control for clipping, adjust the volume of the source (i.e., amplifier, mixer, or tapecorder) until the red light or dot no longer appears in the Recording level window. You can also control the volume using the input or volume controls in the Recording level window. Sound Edit does not recommend this method because the sound quality may be sacrificed.

Creating a new sound file

1. Load your cassette into the tape recorder.
2. Plug your headphones or speakers into the headphone jack in the computer.
3. Adjust the volume on your tape recorder.
4. To check volume start the tape without recording in your computer's program.

5. Adjust volume as needed on both sides.
6. Remember to rewind the tape to the beginning before going to the next step.
7. Press the play button on the tape recorder.
8. Press the record button in the Sound Edit control window.
9. Make sure to monitor the sound in the record Levels window for clipping.

"Supplemental Report to Diary 53, Networking the Sound Digitizing Device," Old Colorado City Communications and the National Science Foundation Wireless Field Tests, October 20, 2002, Lansing, Michigan, ttp://wireless.oldcolo.com/biology/ProgressReports2002/Progress%20Reports2002/53SupplementalReport(10-20-02).htm

Old Colorado City Communications
and the
National Science Foundation
Wireless Field Tests

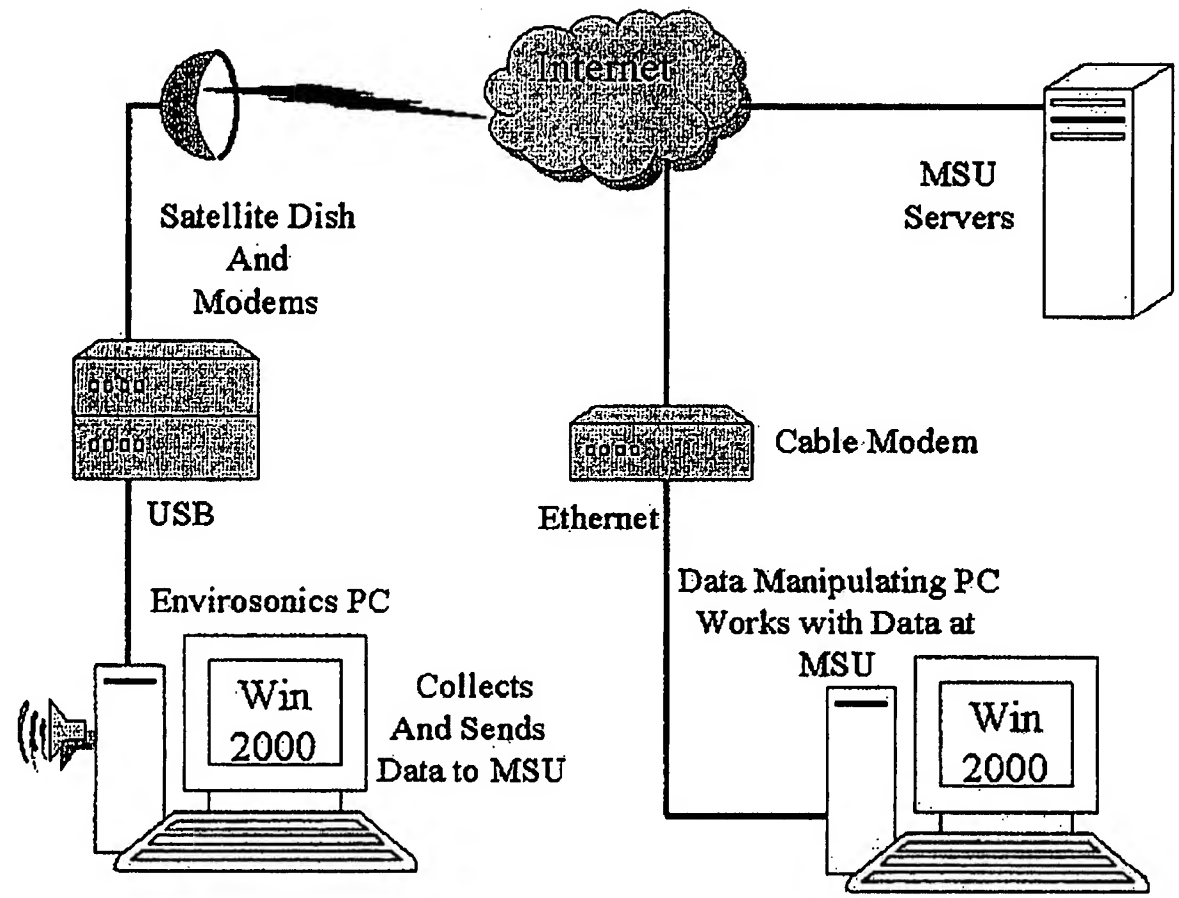
Supplemental Report to Diary 53

Networking the Sound Digitizing Device

October 20, 2002

Lansing, Michigan

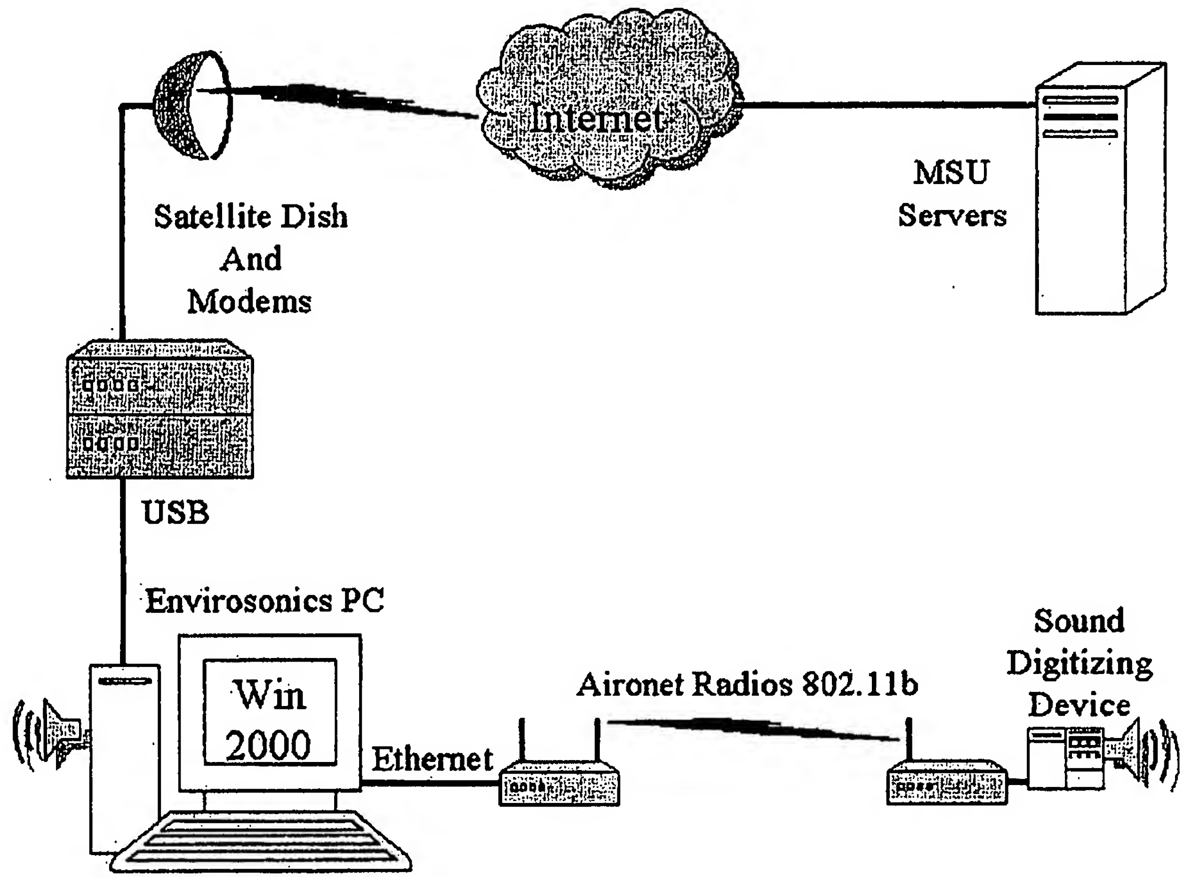
The networking portion of the prototype Sound Digitizing Device installation is explained in the following text. Our goal included working within the operational confines of the existing network architecture, currently supporting previous envirosonics related research. The existing network included a Satellite feed via a DirecPC two-way communications Internet link and a two-way communications Internet link via a local cable modem service. See the network diagram below:



The desired method of communications to the MSU server was through the DirecPC satellite system to best emulate a field installation. However, the satellite system was not designed to provide the generic network connectivity we needed. The satellite system we were working with was designed to work with a standard desktop PC running proprietary satellite networking support software through a USB interface. The satellite system supported the sound capturing PC being used as office level model for this research, and could not be disturbed. The network IP from the satellite feed is also a non-routable private IP address, so getting to the Sound Digitizing Device system for updates and changes would not be easy. Networking the Sound Digitizing

Device prototype on the satellite feed would be a difficult and messy networking job, further complicated by the satellite feed line to the PC being based on a USB link rather than Ethernet.

To provide the digital audio data to the satellite, we would have to dual home the win 2000 PC and utilize an Ethernet network card to provide a network link between the win 2000 system and the Sound Digitizing Device. See Below:



This was the network topology after our first visit to Lansing to install the SDD. It provided the connectivity between the SDD and the Envirosonics PC. However, it did not provide access from the Internet to the SDD directly.

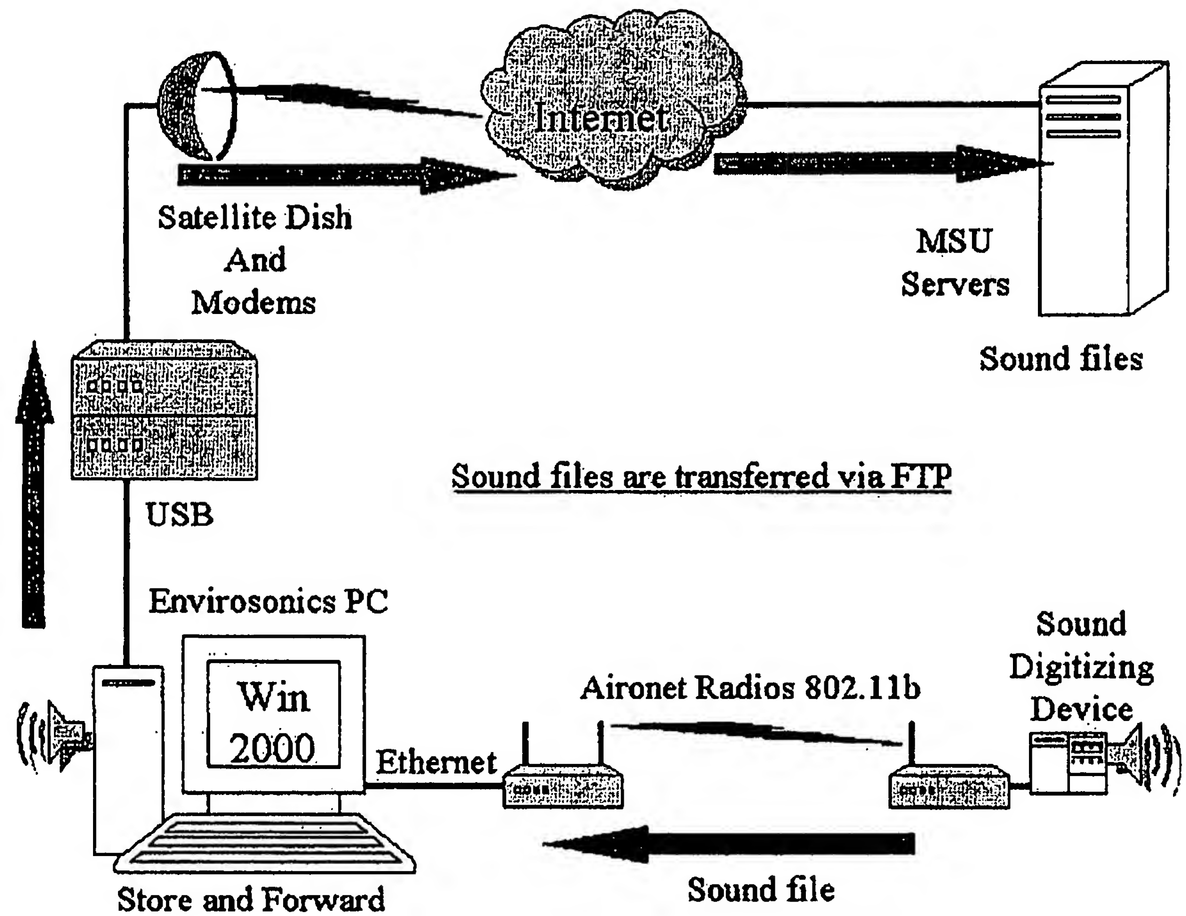
The flow of sound data starts at the SDD at the lower right. The sound is recorded digitally and stored locally on the SDD utilizing a program called LAME to rip files from the live-ice generated stream. The sound data is also provided as a live audio stream that can be monitored on the Envirosonics PC using a program such as WinAmp. However, the recorded file stored locally on the

SDD is transferred to the Envirosonics PC via the network link provided by two Aironet 2.4 GHz ISM band DSSS radios. Both the Envirosonics PC and the SDD connect to the Aironet radios via Ethernet. The file is transferred and named according to a scheme, which denotes the day and hour, but is completely configurable. A copy of the ftp'd file is then transferred from the Envirosonics PC to the Internet through the DirecPC satellite to an MSU server via FTP. A unique program, existing in the Unix environment for many, many years called "Expect" is utilized to mimic a user typing command line arguments into a program interface. In other words, "Expect" is a programmed virtual user inside the SDD that interacts with the ftp program to initiate the ftp session to the Win 2000 machine. An expect script is quite simple;

```
Send "FTP 192.168.0.1"
Expect "login"
Send "MyUserName"
Expect "password"
Send "MyPassword"
Expect "ftp >"
Send "bin"
Expect "binary"
Send "put stream10-21-1230"
Expect...
```

The expect program is able to interact with a great many programs, making it a very powerful tool to perform house-keeping within a computer system, special tasks, such as we are using, and can even perform decision making in many forms.

The network path of the sound files transferred via ftp is shown below.



A few problems remain after the implementation shown above:

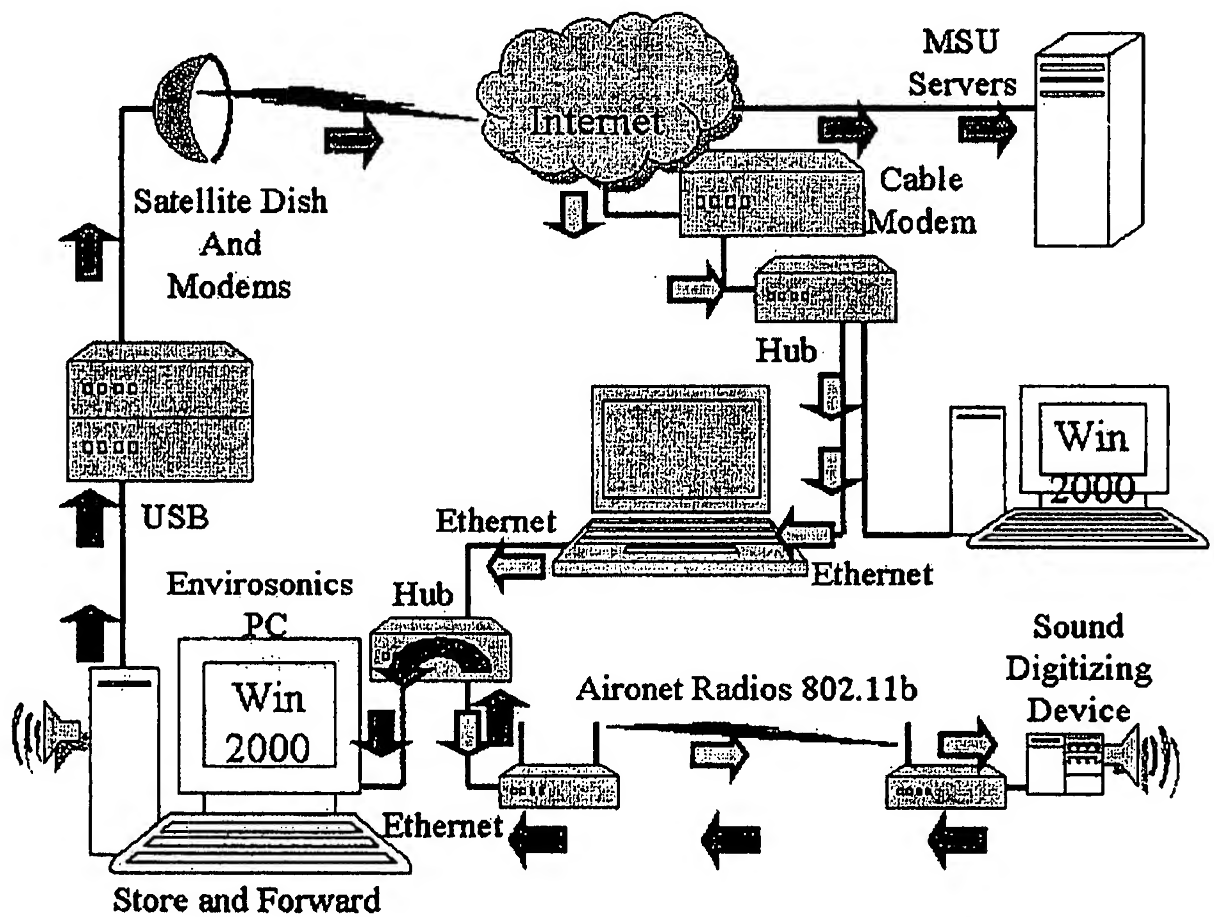
- **No remote access could be provided through the DirecPC Satellite connection for updates or adjustments.**
- **No streaming outside of the Envirosonics PC could be accessed.**
- **Win 2000 machines do not make the best Internet gateways, especially when one interface is a USB port talking to a satellite via proprietary means.**

· The IP addresses used within the DirecPC network are not routable from outside the DirecPC network. This could be alleviated via a virtual tunnel to a trusted remote machine.

To alleviate the problems as easily as possible, we looked at the Cable Modem side of the network. Our solution to the problem was to install a gateway system that does NOT route packets, but rather has access to both networks. The gateway system chosen was an IBM Thinkpad system running Redhat Linux 7.3, using two Ethernet interfaces. One interface would connect to the Satellite network, and the other interface would connect to the Cable Modem network.

If you follow the yellow arrows, you will see the path used for remote management of the SDD, which allows connections from one network to the other network, but not in a routed fashion. You must log into the laptop acting as a gateway between the two networks to access the other network. If you follow the maroon arrows, you will see the ftp path for the audio files discussed earlier.

Yellow Arrows: Remote Management
Maroon Arrows: Audio File Transfer Path



To provide an added security measure, both the laptop in the middle of the picture above and the Sound Digitizing devices utilize Secure Shells (SSH). The secure shell is accessed via a program called "Putty" which exists in the public domain and runs under Windows. You open up the SSH program "Putty" and select the SSH connection to the appropriate IP address. After authentication, the SSH program allows access to the system as if it were a telnet session. Most other sockets or ports on the Thinkpad laptop and the SDD have been shut down to provide fewer opportunities to be hacked.

The laptop was picked for the gateway for several reasons, such as:

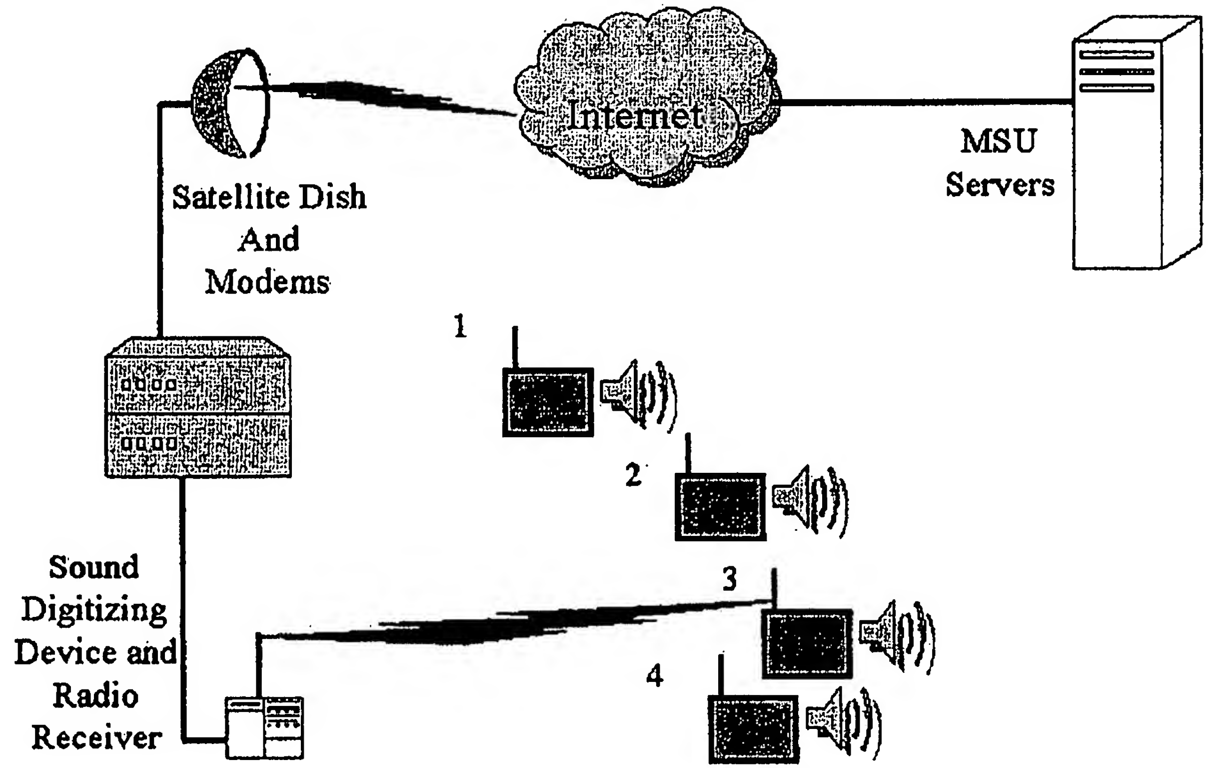
1) Linux is known to run well and install easily in the IBM Thinkpad systems, and since this was a remote install with a time crunch, things needed to go smoothly.
2) A laptop has automatic battery backup when the 110V AC power fails.
3) The size is small and the CPU power more than adequate for the intended use, as well as possible future streaming use.
4) Linux is very network friendly, easily configured multi-network operating system, so this provides a reliable access method in a true multi-user environment.

The SDD system provides several functions over and above the command line interface. Since the typical biologist is not a network guru, we have provided a "point & click" interface via a web-based tool. This tool is called "Webmin" which is easily configured to provide a point & click interface to many lower level Linux programs. From this interface you can manipulate IP addresses, or which programs run or listen to sockets, configuration of programs, configuration of users, etc. It makes Unix administration as easy as that of a Windows based machine. Webmin has the added ability of being changed when something does not do what you would expect, or you could write your own simple tool to provide the manipulation of some parameter not readily offered in the pre-packaged Webmin interface.

Another web-based interface is provided by the streaming software. By accessing a specific port on the SDD via a standard browser, you can look at the history of recorded digital sound tracks previously transferred to the server system. This interface can provide another way to access the data recorded by the SDD for use other than the routine use it was designed for. You can also force a recording if an event was happening in the area that would provide interesting data, such as the sound of a storm, a migration of birds, or man made sound events.

Keep in mind the complexity of the network shown in the previous network diagrams does not reflect a field deployment of a SDD, but rather to fit the SDD prototype within the confines of an existing network. The actual network implementation should be designed in advance to facilitate the needs of the device and all humans that will support the system, while targeting simplicity for a main goal. Below are two examples of what a field deployment might actually look like:

Example 1: Using "Smart Sensors" with IP all the way to the sensor:



A cost effective approach using "less smart sensors" which send audio
Via FM or some means preserving fidelity to the Sound Digitizing Device
In a time multiplexed method

In the design immediately above with "Less smart - smart sensors", another not-so-obvious parameter was alleviated: "Power". By using very simple circuits as the acoustical sensors, and the digitizing done in only one place, the need for fairly large amounts of power is greatly alleviated. To follow this power reduction effort even further, a far more simple SDD could be designed such that the digitization takes place within a DSP (Digital Signal Processor) Integrated Circuit (IC) programmed to perform this function and requiring far less power than any off-the-shelf device we have available to us at this time.

Conclusion:

The network additions performed to facilitate this prototype installation were quite creative and reaching for opportunities to manipulate the network as passively as possible, while providing the connectivity desired. The operational design from the SDD viewpoint reflected a desire to provide capabilities we would like to have in a true field installation designed for envirosonics research. We achieved all of the goals for the prototype, some of which were formal requirements, and others which were "would it be neat if...." desired modes of operation. We have shown several network designs, with examples of what would be far more simplistic in implementation, along with ideas of the next generation Sound Digitizing Devices that would facilitate envirosonic research completely.

Michael Willett
Senior Technical Assistant and Collaborator

PREVIOUS

Chronological Progress Diaries | Purpose | Scope | Participants
Project Plan | Regulatory Issues | LTER | Top Page

"Macromedia SoundEdit 16 Support Center-Working with Other Programs, What is Shockwave Audio Streaming?"http://www.macromedia.com/support/soundedit/how/shock/whatis.html

Home / Products / **SoundEdit 16**

Macromedia SoundEdit 16 Support Center

Working with Other Programs

What is Shockwave Audio streaming?

What we mean by "streaming audio" is that the sound is delivered to you as it is being received from the web site that you are visiting. This is very different from downloading a file to your hard drive and then playing it after the entire file has been downloaded. The advantage of streaming is that there is no waiting (or very little) from the time you click the mouse until you hear the sound.

Audio is very information intensive -- it takes a lot of data to represent a sound accurately. On the other hand, even a very fast modem processes data at a relatively slow rate. (Think of it as a big stream of water being pushed through a tiny pipe.) Because of this, it is necessary to compress the audio so that it can be squeezed through the modem to be played back at an acceptable quality. Shockwave Audio uses very sophisticated mathematical analysis to compress the sound so that it can be represented by relatively few bytes of data. This much smaller data stream is sent through your modem, uncompressed in your computer, converted back into audio, and then played through your speakers.

Shockwave Audio is scaleable, which means that you can select the quality level to use for the audio. Be careful when making this choice -- a very high quality setting may contain too much information to squeeze through a modem in real-time. In this case, users may hear gaps in the playback. For example, if you want people with 28.8k modems to stream successfully, limit your SWA files to lower quality settings. However, if you know that the audio is intended for user's on a high-speed network such as a corporate intranet, you can use the highest quality settings with very good results.

"Chapter 3: Overview," last updated December 2, 1999,http://service.real.com/help/library/guides/g270/htmfiles/overview.htm

Chapter 3: Overview

Welcome to RealServer, the streaming media solution! RealServer streams audio, video, image, animation, text, and other data types. RealServer also allows you to grow with your changing needs. This chapter introduces RealServer concepts and features.

To begin serving right away, consult Chapter 1, "Quick Start".

What Is RealServer?

RealServer is software that streams media-both pre-recorded and live events-over a network. The client receives the media in real time, and does not have to wait for the clip to download.

Components of RealServer

RealServer software consists of the following components:

- **Executable**-RealServer's main software, called `rmserver.exe` for Windows platforms, and `rmserver` for UNIX platforms.
- **Plug-ins**-these files provide the functionality of RealServer's individual features. Because of this open architecture, third parties can create custom features, allowing you to extend the abilities of your RealServer.
- **Configuration file**-a text file, based on XML format, that stores all of your RealServer's customized information. The configuration file name is `rmserver.cfg`.
- **License file**-one or more files which control the features enabled in your **RealServer**.
- **RealSystem Administrator**-a Web-based console for customizing and monitoring your RealServer.
- **Tools**-additional software tools such as the Java Monitor, which allows you to view how many clips are being served at a given time, and G2SLTA, which broadcasts pre-recorded clips as if they were live events.
- **Other files**-depending on the particular RealServer package you purchased, your installation may have other files that perform additional functions, such as commerce or ISP hosting.

What is RealSystem?

RealServer is a member of the RealSystem G2 family of software tools. Three components make up RealSystem G2:

- **Production tools**-such as RealProducer Pro or RealProducer Plus that create media (such as audio, video, or animation)
- RealServer-which streams media
- **Client software**-such as RealPlayer, which plays the streamed media

The following diagram provides an overview of how RealSystem components work together.

RealSystem Components

Production Tools

The person who designs the content that you serve from your RealServer uses production tools to create the content. These tools convert audio, video, or animation to a data type format that RealServer can stream.

The content creator may additionally create a SMIL file to synchronize several clips in a single presentation. A SMIL file coordinates the playing and layout of media clips in parallel or sequence.

Since RealServer is able to deliver many formats, there are many tools that can be used in creating content. Production tools can optimize the material for delivery over the Internet, based on the content of the material and the expected capabilities of the users' equipment.

The content creator can prepare media clips in advance, or can encode a live event as it happens. In this manual, we use the generic term "encoder" to describe the software (such as RealProducer) that converts media or events into a format that RealServer can deliver.

RealServer

Just as a Web server delivers pages to Web browsers over the Internet, RealServer serves media clips, created with the production tools described earlier, to clients. It allows users to stream, rather than download, the media clips. By streaming the content, the user can begin to watch the clip almost immediately and does not have to wait for the entire file to download.

Client Software

A client such as RealPlayer plays the streamed media.

Other Software

In addition to the RealSystem G2 software, you may work with additional optional software, such as:

- Web server
- Web browser
- Firewalls
- Networking software
- Database software, if commerce authentication features are in use
- Ad server or services, if advertising features are in use

How RealServer Works

RealServer streams media to clients over networks and the Internet. It is usually employed in conjunction with a Web server. Some RealServer features can interact with third-party products to create specialized functions, such as report analysis.

Channels and Protocols

RealServer uses two connections, known as "channels," to communicate with clients: one for communication with the client, and one for actual data. The communication channel is known as the "control channel," since it is over this line that RealServer requests and receives passwords, and the client sends instructions such as fast-forward, pause, and stop. Media is actually streamed over a separate "data channel".

Every link to content begins with a protocol identifier, such as `rtsp`, `pnm`, or `http`.

RealServer uses two main protocols to communicate with clients: RTSP (Real Time Streaming Protocol) and PNA (Progressive Networks Audio).

Occasionally, RealServer will use HTTP for metafiles that point to RealServer content, and for the HTML pages served by RealServer (such as the Web-based RealSystem Administrator). It may also be used in delivering clips to clients that are located behind firewalls.

Within these channels, RealServer uses two other protocols for sending instructions and data:

- TCP-sends commands from the client such as "start" and "pause," and from RealServer to clients for information such as the clips' titles
- UDP-sends the actual data

See Chapter 9, "Firewalls and RealServer" for more detailed information on RealServer's use of ports.

Occasional Exceptions

Because many firewalls are configured to allow only TCP connections or HTTP traffic, you may need to make some adjustments to receive data from an encoder or to work with clients if there is a firewall between it and your RealServer. See Chapter 9, "Firewalls and RealServer".

Communication Between Encoder and RealServer

When the encoder connects to RealServer and sends encoded media data, it uses a one-way (UDP) connection to communicate with RealServer.

UDP Connection Between Encoder and RealServer

Some firewalls do not permit UDP packets, so RealNetworks encoding software such as RealProducer has a setting that uses TCP connections to send the same encoded media, since many firewalls allow TCP traffic.

TCP Connection Between Encoder and RealServer

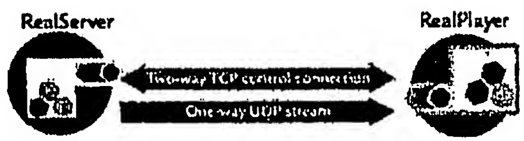
Communication Between RealServer and RealPlayer

When the user clicks a link that points to a media presentation, RealPlayer opens a two-way connection with RealServer. This connection uses TCP to send information back and forth between RealPlayer and RealServer.

Initial TCP Control Connection

Once RealServer approves the request, it sends the requested clip along a one-way UDP channel.

UDP Data Connection



As it receives the streamed clip, RealPlayer plays it at high fidelity.

Streaming Delivery Methods

There are two main ways for controlling how a user experiences a clip:

- **On-demand**-like renting a video at a 24-hour video store, the clip is available to the user whenever she wants. The user can fast-forward, rewind, pause, and RealServer sends the right part of the clip. This type of clip is pre-recorded or pre-assembled.

- **Live**-like a live telecast of the Olympic Games, users tune in to the action that is happening now. A user can't fast-forward or rewind through the clip, because the event is happening in real time. To deliver content as a live event requires that there actually is a live event, and that you or the content creator have the software and hardware to capture it and convert it to a media format that RealServer can broadcast.

A third method, which uses on-demand clips but delivers them as if they were live, is available. It is not used as commonly.

- **Simulated live**-Just as a television broadcaster might record a live event and broadcast it later, such as Olympic sports that wouldn't be seen because of time zone differences, simulated live broadcasts take a pre-recorded event and broadcast it as a live event. Thus, although it is pre-recorded, users view the event as if it were live.

The table below summarizes the three participation types.

User Participation Comparisons

On-Demand (through Streaming)	Live Delivery (through Unicasting, Splitting, or Multicasting)	Simulated Live Delivery (through Unicasting, Splitting, or Multicasting)
Can access presentations any time.	Can only access presentations while they're in-progress.	Same as live delivery.
Files are stored on disk.	Presentations don't exist as files.	Same as on-demand delivery.
Presentations always begin streaming at the beginning of the file.	Everyone sees the same part of the presentation at the same time-late-comers join in the middle.	Same as live delivery.
User can fast-forward through the clip or pause it at any point.	User plays the clip all the way through.	Same as live delivery.
Similar to a videotape of past Olympic event highlights.	Similar to live television coverage of an Olympic event.	Similar to a previously recorded Olympic event, delayed on television because of time zone differences.

Which Delivery Method Is Right for Me?

Once you have determined how you want the user to experience the clip (as on-demand or live), you choose which delivery method you will configure RealServer to use.

- **On-demand**-the choice is simple: streaming is the only delivery method.
- **Live and simulated live**-there are three ways to deliver the clip: unicasting, splitting, and multicasting.

On-Demand Streaming

Pre-recorded clips are delivered through a method called streaming. A user who clicks a link to an on-demand clip watches it from the beginning. The user can fast-forward, rewind, or pause the clip. See Chapter 10, "Streaming On-Demand Presentations".

Live Event Broadcasting

Live clips can be delivered in several different ways. As the administrator, you will decide which method to use based on your network needs. A user who clicks a link to a live clip joins the live event in progress; fast-forward, rewind, and pause are not available because the event is happening in real time.

Live clips are broadcast as they are created. These clips don't exist as files, since they are created as the live event happens. Live content can be saved into files through the live archiving feature; the archived files become on-demand content and are handled as such.

Unicasting

This is the simplest and most popular method for live broadcasting. It requires little or no configuration. Refer to Chapter 11, "Unicasting Live Presentations".

Splitting

Splitting is a term to describe how one RealServer can share its streams with other RealServers. Clients connect to these other RealServers, called splitters, rather than to the main RealServer where the streams originate. Splitting reduces the load on the source RealServer, leaving it free to distribute other broadcasts. This method moves the broadcasts closer to clients, improving the quality of service for them. See Chapter 12, "Splitting Live Presentations".

Multicasting

Multicasting is a standardized method for connecting large numbers of users with presentations delivered over a network or the Internet. Consult Chapter 13, "Multicasting Live Presentations".

Simulated Live Event Broadcasting

The same delivery options are available as for live broadcasting: unicasting, splitting, and multicasting. The only difference is that the event has already been recorded, and no connection to a production tool or encoder is needed. The G2SLTA program, included with RealServer, sends the on-demand file to RealServer as if it were a live event. See "Creating a Live Source with G2SLTA".

Summary

The following table shows the user participation styles and the accompanying delivery methods.

Comparison of Delivery Methods

User Participation	Delivery Method	Appropriate Use	Requirements
On-demand	Streaming	Presentations that are limited to the number of licensed connections, CPU speed, amount of RAM, and available bandwidth of a single machine.	Requires sufficient bandwidth to handle the number of clients connecting.
Live and simulated live	Unicasting	Broadcasts that are limited to the number of licensed connections, CPU speed, amount of RAM, and available bandwidth of a single RealServer machine.	Requires sufficient bandwidth to handle the number of clients connecting.
	Splitting	Broadcasts that are limited to the number of licensed connections, CPU speed, amount of RAM, and available bandwidth of all RealServer machines.	Requires at least two RealServers. Must configure source RealServer and splitter RealServers.
	Multicasting	Broadcasts that will be viewed by unlimited users around the globe on a multicast-enabled network.	Requires a multicast-enabled network. Can be combined with splitting to cover a greater geographical region where networks are not multicast-enabled.

In some cases, you can use more than one live delivery method at once, to reach the maximum number of users while minimizing network bandwidth.

- The combination of splitting and multicasting is described in "Splitting and Multicasting".

- The combination of unicasting and multicasting is described in "Requiring Multicast Access Rather than Unicast" (for back-channel multicast) and "Using Unicast as a Backup Method" (for scalable multicast).

Linking to RealSystem Content

Links to media clips served by RealServer have several components that tell RealServer how to serve the clip and where to look for the clip.

Content creators will put most links into Web pages. A user looking at a content creator's site will click the link, and through the process described in "How RealServer Works", will receive the media.

For example, the following link for a RealVideo file would appear in a Web page (the URL for the media clip is shown in bold):

```
<a href="http://realserver.company.com:8080/ramgen/Concerts/French/
debussy.rm">Click here to watch today's concert!</a>
```

The clip may be pre-recorded, live, or pre-recorded but delivered as live.

Additional Information
Instructions on creating links to RealSystem clips are described in depth in Chapter 5, "Understanding Link Formats".

Working with Other Webcasting Professionals

This manual assumes that you (the RealServer administrator) are managing your RealServer, and that a second person (the content creator) is making media clips and SMIL presentations and putting links in Web pages. In reality, you may be filling both roles, especially when you are setting up a feature and want to do some quick tests. But it makes it easier to discuss the roles when they are described as separate people.

The RealServer administrator needs to provide the content creator with certain information, so that she can create the correct links in her SMIL files and Web pages. If the content providers are encoding live material, they will need to know where to direct their live data.

Responsibilities of RealServer Administrator and Content Creator

RealServer Administrator	Content Creator
Configures and maintains RealServer	Performs encoding or assembles presentations
Supplies information needed to create links	Creates links

Content Creators of On-Demand Content

Content creators will need the following information:

- Location where they should place their files
- Address or name of RealServer
- Port numbers for each protocol (but only if you have changed them from the recommended default settings)
- Information about whether Ramgen is in use (Ramgen is defined in "Ram Files and Ramgen" in Chapter 5, "Understanding Link Formats".

Content Creators of Live Content

In order to encode a live stream to RealServer, content creators need to know this information:

- Address or name of RealServer
- Port number to connect to
- Authentication information such as passwords (if any)
- URL to use in Web pages that point to a live broadcast or multicast
- URL to use in a SMIL file

Other RealServer Administrators

RealServer can broadcast to other RealServers, which can redistribute the presentations to clients, thus reducing the load on the original RealServer. This feature is called splitting. If you are working with the administrator of the other RealServer (the splitter), you will need to give that person certain information about your RealServer settings. That information is outlined in Chapter 12, "Splitting Live Presentations".

Firewall Administrators

If there are users within your network that either cannot receive presentations from RealServers on the Internet or who receive poor quality streams, information in Chapter 9, "Firewalls and RealServer" will help the firewall administrator understand what changes can be made that will enhance the users' experience.

Network Administrators

In determining both how much bandwidth is available on your network, and how much is appropriate for RealServer to use, network administrators can help you arrive at suitable numbers.

RealServer Features

In addition to the delivery methods described earlier in this chapter, RealServer has other features that help you administer your RealServer.

RealSystem Administrator

RealSystem Administrator is the Web-based console for customizing RealServer features. It can be run from any browser on your network. It is password-protected when first installed, and you can create additional user names and passwords for any other people who will be helping you administer your RealServer.

Access Control

The access control feature lets you associate certain client addresses with the ability or permissions to connect to certain ports.

Authentication

Authentication verifies the identity of a user or RealPlayer that is making a request for streamed media. The verification can come in the form of asking for a name and password, or it can be hidden from the user.

ISP Hosting

RealServer works with your existing user accounts and directory structure to make users' media files available for streaming. You allocate a minimum and maximum number of connections for each account, based on the number of streams permitted by your license. Allocating on a per-connection basis, rather than by stream, ensures that all files, including SMIL files which reference multiple streams, will always be served.

Monitoring

RealSystem Administrator includes a real-time Java Monitor to show activity on your RealServer, making Server management easy. It shows who is using the Server, when it is most used, and which files are the most requested, as well as other information.

Reporting (Log Files)

RealServer can create reports of historical data that let you see trends and gather information. Track who visited your site and for how long; what clips they watched and whether they watched them all the way through to completion. This information is stored in the access log. Any error messages are recorded in the error log. Requests for streams which will be cached are stored in the cached requests log.

Ad Streaming

RealServer can dynamically insert ads into streaming presentations. Offering integration with any HTML-based ad serving system, RealServer uses SMIL (Synchronized Multimedia Integration Language) to lay out ads and requested content in RealPlayer. This chapter explains how to set up RealServer's ad streaming features.

RealProxy

RealProxy is software that stores streamed media. While it is not part of RealServer, it can work with RealServer to share the distribution load, thereby conserving bandwidth over an intranet and allowing RealServers to send streams to a wider audience. It is generally installed on an intranet or on a large Internet Service Provider (ISP). When a client on the intranet or hosted by the ISP requests a streamed media file, RealProxy intercepts the request and sends it on behalf of the client. RealProxy then stores the requested media and streams it to any other clients who subsequently request the same material.

Firewalls

Firewalls are not specifically a RealServer feature, but they are important in networked environments. A firewall is a software program that monitors, and sometimes controls, all transmissions between an organization's internal network and the Internet. A network can consist of a company's local area networks, wide area networks, and the Internet, or it can be just an Internet Service Provider preventing inappropriate access to the files of its customers. The firewall's role is to ensure that all communication, in both directions, conforms to the organization's security policies.

Using RealServer Features Together

RealServer components can be combined to conserve bandwidth and deliver high-quality presentations. The table below summarizes RealServer features and how they work together.

For additional information on exactly how any of these features work together, refer to the chapter that describes the feature.

Interoperability of RealServer Features

	Streaming	Unicasting	Archiving	Simulated Live	Push Splitting	Pull Splitting	Back-Channel Multicasting	Scalable Multicasting	RealProxy Access	Firewalls[1]	Access Control	Authentication
On-Demand Delivery												
Streaming	-	-	-	-	-	-	-	-	-	-	-	-
Live Delivery												
Unicasting	-	-	-	-	-	-	§	§	-	-	-	-
Archiving	-	-	-	§	-	-	§	§	-	-	-	-
Simulated Live (G2SLTA)	-	-	§	-	§	§	§	§	-	-	-	-
Splitting-Push	-	-	-	§	-	§	§	§	-	-	-	-
Splitting-Pull	-	-	-	§	§	-	§	§	-	-	-	-
Multicasting-	-	§	§	§	§	§	-	-	-	-	-	-

Back-Channel												
Multicasting-Scalable	-	§	§	§	§	§	-	·	-	·	·	·
Other Features												
RealProxy Access	·	-	-	-	-	-	-	-	·	-	·	·
Firewalls[1]	·	·	-	·	·	·	·	·	-	·	·	·
Access Control	·	·	·	·	·	·	·	·	·	·	·	·
Authentication	·	·	§	·	·	·	·	·	·	·	·	·
ISP Hosting	·	-	-	-	-	-	-	-	·	·	·	-
Monitoring	·	·	-	·	·	·	·	-	-	-	·	·
Reporting (Log Files)	·	·	-	·	·	·	·	§	·	-	·	·
Ad Streaming	·	·	-	·	§	§	§	§	·	·	·	§

· Features work together automatically; no additional configuration required beyond normal setup

§ Requires some special considerations for these features to work together

- Not applicable; features are unrelated

[1] Firewall information assumes that firewall allows streaming media traffic and multicast traffic

For information on RealNetworks' technical support, click here.
Comments on this document? Click here.
This file last updated on 12/02/99 at 10:52:53.

"How Internet Radio Works," Howstuffworks,
http://computer.howstuffworks.com/internet-radio.htm/printable

How Internet Radio Works

by Debra Beller

A college student in Wisconsin listens to a disc jockey in Jamaica play the latest rapso (calypso rap) music. A children's advocacy group unites its geographically diverse members via private broadcast. A radio listener hears an ad for a computer printer and places an order immediately using the same medium on which he heard the ad. All of this is possible with Internet radio, the latest technological innovation in radio broadcasting since the business began in the early 1920s.

Internet radio has been around since the late 1990s. Traditional radio broadcasters have used the Internet to simulcast their programming. But, Internet radio is undergoing a revolution that will expand its reach from your desktop computer to access broadcasts anywhere, anytime, and expand its programming from traditional broadcasters to individuals, organizations and government.

In this edition of **HowStuffWorks**, we'll explore the Internet radio revolution in terms of equipment, transmission, programming and the alterations in the listener/broadcaster relationship.

Freedom of the Airwaves

Radio broadcasting began in the early '20s, but it wasn't until the introduction of the transistor radio in 1954 that radio became available in mobile situations. Internet radio is in much the same place. Until the 21st century, the only way to obtain radio broadcasts over the Internet was through your PC. That will soon change, as wireless connectivity will feed Internet broadcasts to car radios, PDAs and cell phones. The next generation of wireless devices will greatly expand the reach and convenience of Internet radio.

Uses and Advantages

Traditional radio station broadcasts are limited by two factors:

- the power of the station's transmitter (typically 100 miles)
- the available broadcast spectrum (you might get a couple of dozen radio stations locally)

Internet radio has **no geographic limitations**, so a broadcaster in Kuala Lumpor can be heard in Kansas on the Internet. The potential for Internet radio is as vast as cyberspace itself (for example, Live365 offers more than 30,000 Internet radio broadcasts).

In comparison to traditional radio, Internet radio is **not limited to audio**. An Internet radio broadcast can be accompanied by photos or graphics, text and links, as well as interactivity, such as message boards and chat rooms. This advancement allows a listener to do more than listen. In the example at the beginning of this article, a listener who hears an ad for a computer printer ordered that printer through a link on the Internet radio broadcast Web site. The relationship between advertisers and consumers becomes more interactive and intimate on Internet radio broadcasts. This expanded media capability could also be used in other ways. For example, with Internet radio, you could conduct training or education and provide links to documents and payment options. You could also have interactivity with the trainer or educator and other information on the Internet radio broadcast site.

Internet radio programming offers a **wide spectrum of broadcast genres**, particularly in music. Broadcast radio is increasingly controlled by smaller numbers of media conglomerates (such as Cox, Jefferson-Pilot and Bonneville). In some ways, this has led to more mainstreaming of the programming on broadcast radio, as stations often try to reach the largest possible audience in order to charge the highest possible rates to advertisers. Internet radio, on the other hand, offers the opportunity to expand the types of available programming. **The cost of getting "on the air" is less** for an Internet broadcaster (see the next section, "Creating an Internet Radio Station"), and Internet radio can **appeal to "micro-communities" of listeners focused on special music or interests.**

Creating an Internet Radio Station

What do you need to set up an Internet radio station?

- CD player
- Ripper software (copies audio tracks from a CD onto a computer's hard drive)
- Assorted recording and editing software
- Microphones
- Audio mixer
- Outboard audio gear (equalizer, compressor, etc.)
- Digital audio card
- Dedicated computer with encoder software
- Streaming media server

Getting audio over the Internet is pretty simple:

1. The audio enters the Internet broadcaster's encoding computer through a sound card.
2. The encoder system translates the audio from the sound card into streaming format. The encoder samples the incoming audio and compresses the information so it can be sent over the Internet.
3. The compressed audio is sent to the server, which has a high bandwidth connection to the Internet.
4. The server sends the audio data stream over the Internet to the player software or plug-in on the listener's computer. The plug-in translates the audio data stream from the server and translates it into the sound heard by the listener.

There are two ways to deliver audio over the Internet: downloads or streaming media. In **downloads**, an audio file is stored on the user's computer. Compressed formats like MP3 are the most popular form of audio downloads, but any type of audio file can be delivered through a Web or FTP site. **Streaming audio** is not stored, but only played. It is a continuous broadcast that works through three software packages: the encoder, the server and the player. The **encoder** converts audio content into a streaming format, the **server** makes it available over the Internet and the **player** retrieves the content. For a live broadcast, the encoder and streamer work together in real-time. An audio feed runs to the sound card of a computer running the encoder software at the broadcast location and the stream is uploaded to the streaming server. Since that requires a large amount of computing resources, the streaming server must be a dedicated server.

Lots More Information!

Related HowStuffWorks Articles

- How Radio Works
- How the Radio Spectrum Works
- How Satellite Radio Works
- How Ham Radio Works

More Great Links

- Radio-Locator: Internet Radio Search Engine
- SaveInternetRadio.org
- Kids Internet Radio
- RadioTower.com Internet Radio Directory

"Telecommunications and Personal Management Services Linked in Collaboration by Verizon and Microsoft," October 23, 2001,http://www.microsoft.com/presspass/press/2001/oct01/10-23MSVerizonPr.asp

PressPass · Information for Journalists

Telecommunications and Personal Management Services Linked In Collaboration by Verizon and Microsoft

Key .NET Technologies to Help Verizon Customers Balance Family and Work Life

NEW YORK and REDMOND, Wash. -- Oct. 23, 2001 -- Balancing family, social and professional responsibilities can be overwhelming, but some innovative work by Verizon and Microsoft Corp. seeks to make the daily juggle much more manageable.

Microsoft and Verizon are exploring new uses of technology to integrate the latest telecommunications services, Verizon e-business applications and select Microsoft® .NET and Windows® XP services to provide customers with additional control over their lives. These technologies include telecommunications and messaging services, calendaring and personal directories. Features of .NET and Windows XP services now offered by Microsoft are playing an important role in one such application currently being tested by Verizon.

With a service bearing an internal code name Digital Companion, Verizon is working to extend the capabilities and features of its telecommunications services, already provided through one of the world's most advanced and pervasive networks.

"Being in a wired world should mean greater productivity and more control for people, and this is a key driver for our efforts," said Shaygan Kheradpir, president of eBusiness for Verizon. "Digital Companion would enable customers to access and use call management features, such as Caller ID, over the Internet, in new and innovative ways."

One version of the Digital Companion will use Microsoft's .NET Alerts to extend the reach of the service for Verizon's customers and will also use the .NET Passport authentication and single sign-in service to provide an easier, faster and more compelling experience.

"This effort is a great example of the kinds of customer relationships that are enabled by .NET," said Sanjay Parthasarathy, senior vice president of the .NET Strategy Group at Microsoft. "Verizon has combined its industry-leading telecommunications services with the smart clients, servers and services that make up the .NET platform to create a truly empowering communications experience for customers."

Anytime, Anywhere Communications

Based on the collaborative efforts of Verizon and Microsoft, this implementation of Digital Companion would provide a new way for people to more efficiently manage their day-to-day communication.

For instance, a Digital Companion user who is a working mother could get a Caller ID notification through an instant message popping up on her desktop computer signaling that her son's school has called her home. Without missing a beat, mom would

Related Links

- **Microsoft Professional Developers Conference Virtual Pressroom**

Transcript:

- Bill Gates Remarks - Oct. 23, 2001

Feature Stories:

- Thousands of Software Developers See .NET Technologies in Action - Oct. 23, 2001
- On Any Device: .NET Goes Mobile With the .NET Compact Framework - Oct. 23, 2001
- Q&A: For Developers, Microsoft Group VP Muglia Says Microsoft is Delivering on .NET Now - Oct. 23, 2001
- Q&A: Helping Developers Create World-Class Software - Oct. 23, 2001
- Partners Find Microsoft .NET Platform Combines XML Interoperability with High-Productivity Development - Oct. 22, 2001

Press Releases:

- Microsoft Previews Global XML Web Services Architecture - Oct. 23, 2001
- Gates Rallies Developers For New Era of Computing - Oct. 23, 2001
- Massive Industry and Developer Support for Microsoft .NET on Display At Professional Developers Conference 2001 - Oct. 22, 2001
- Microsoft and Trans World Entertainment Announce Broad-based Business, Technology and Marketing Alliance To Deliver Enhanced Shopping Experience For FYE Customers - Oct. 22, 2001

Microsoft Resource:

- Microsoft .NET Web Site

open her Digital Companion and find out that the school has left her a voice message.

By listening to her voice mail, mom would learn that her son is ill and needs to be picked up early. Rather than digging through her address book to find the number of the school, mom scans her caller ID list in her Digital Companion and calls the school to ask if her son requires immediate medical attention.

The school tells her not to worry; her son will be fine, but needs to be picked up early from school. Since critical business calls are expected that afternoon, mom could return to her Digital Companion and forward all her calls to her cell phone just before she leaves to get her son.

Finally, mom could prepare for spending the next day at home and the doctor's office by directing certain important calls to her cell phone and others to her home office. Her family commitments are met, and she never misses a beat with her work.

Utilizing key .NET technologies, Digital Companion would enable a user to remotely access features of Verizon's existing call management services, such as Caller ID and voice mail, any time, anywhere and from virtually any device. With Digital Companion, customers would no longer have to check in at home or work when traveling. Instead, using the remote access to call forwarding provided through Digital Companion, calls could be routed to a cell phone, hotel room or temporary office for the duration of the trip, providing an unprecedented level of convenience for participating customers. Verizon Caller ID lists could also be checked remotely for the first time using this service. Verizon plans to conduct technical trials of Digital Companion in the near future.

Additional Collaboration

While Verizon and Microsoft have worked together in the past, the collaboration around the Digital Companion project is a unique example of the companies' focus to create new services that transform the customer experience. This initiative uses the technical advancements from Microsoft and Verizon, by integrating e-business, telecommunications and software infrastructure to build products that can form the basis for a new generation of communication experience.

Verizon uses Windows 2000 and Microsoft SQL Server (TM) 2000 in several of its key customer relationship management systems. These technologies have enabled Verizon to further enhance the customer experience and resulted in development productivity and improved system performance.

In addition, Verizon and Microsoft are working together to deliver cutting-edge services to Web users by making Verizon's SuperPages.com directory services available on the MSN® network of Internet services. And, recently, Verizon and Microsoft announced an agreement for Verizon to provide broadband digital subscriber line (DSL) access to MSN Internet Access customers.

About Verizon

Verizon Communications (NYSE:VZ) is one of the world's leading providers of communications services. Verizon companies are the largest providers of wireline and wireless communications in the United States, with 125 million access line equivalents and more than

28 million wireless customers. Verizon is also the world's largest provider of print and online directory information in the world. A Fortune 10 company with about 260,000 employees and more than $65 billion in annual revenues, Verizon's global presence

extends to 40 countries in the Americas, Europe, Asia and the Pacific. More information on Verizon can be found at http://www.verizon.com/.

About Microsoft

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and Internet technologies for personal and business computing. The company offers a wide range of products and services designed to empower people through great software -- any time, any place and on any device.

Microsoft, Windows and MSN are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Note to editors: If you are interested in viewing additional information on Microsoft, please visit the Microsoft Web page at http://www.microsoft.com/presspass/ on Microsoft's corporate information pages.

"Real-Time Collaboration Integration in the Portal," T. Odenwald, SAP Design Guild,http://www.sapdesignguild.org/editions/edition5/synch_collab.asp

print version of the article

Real-Time Collaboration Integration in the Portal

By Thomas Odenwald, SAP Labs, Palo Alto

An article in the *Financial Times* of July 12, 2002 stated: "Bill Gates had complained this year that his documents, e-mail, and instant messaging buddy list did not work together and were not related to his calendar."

We could certainly help Mr. Gates with our new solution for the *SAP Collaboration Room* (Enterprise Portal Edition). Not only do we enable single point of access for document management within teams and projects, provide synchronization with the users groupware solutions, and offer unified calendar functionality, we also enable real-time collaboration integration through our own integrated solution, as well as through integration of third-party service providers.

What is Real-Time Collaboration?

The classical real-time collaboration scenarios are:

- Desktop sharing
- Application sharing
  Share applications, documents, or desktop to enable online meetings, remote support, and so on.
- Co-browsing
  Share browser (see application sharing)
- Buddy list and awareness
  A user's ability to maintain a list of people that are the ones he/she usually interacts with and to be able to see which of them is currently online, offline, busy, and so on.
- Whiteboard collaboration
  The electronic equivalent of a blackboard and chalk, but between remote users. Whiteboard systems allow network participants to simultaneously view one or more users writing on an on-screen blackboard or running an application.
- Instant messaging (IM)
  The ability to exchange immediate messages with connected buddies
- Chat service

An enhancement to IM where multiple users can exchange information while still being able to see previous messages

Additional features have emerged recently like

- Voice over IP (two-way audio transmission)
- Video and audio conferencing capabilities
- Annotation tools

Recent terrorist threats and the economic situation are encouraging many companies to take a closer look at these features to avoid unnecessary travel, decrease overall expenses and face-to-face time, lower cost of ownership, and increase productivity. Increasing bandwidth and cheaper hardware makes these tools more attractive by the day.

Gartner Group even predicts that *instant messaging* will overtake classical e-mail in the near future (cf. magazine 15/01).

The tremendous value of Web-based real-time interactivity is not in doubt, especially where responses are needed immediately, consensus time needs to be reduced, and the decision makers are distributed around the globe.

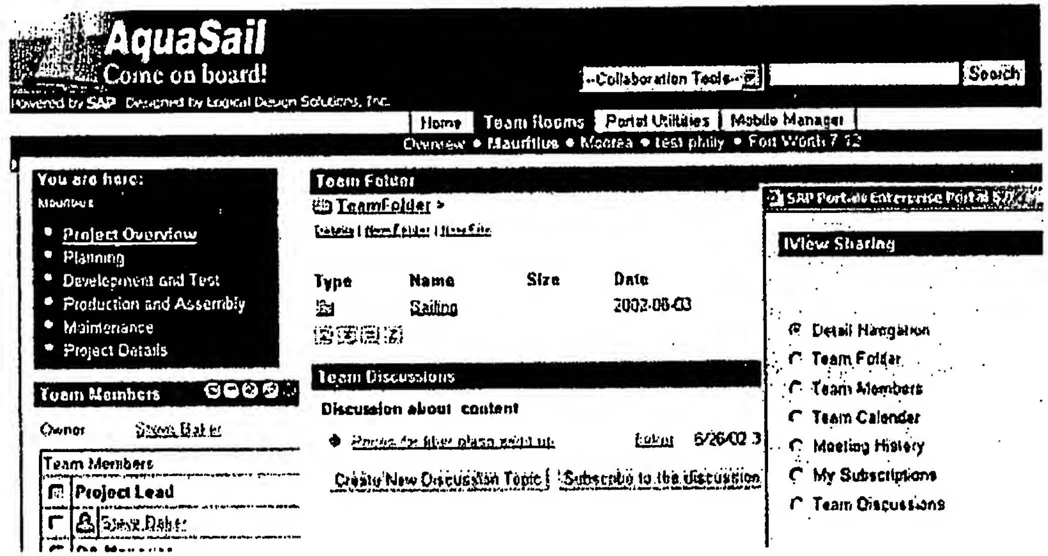
There are lots of options that enable both individuals and teams in different locations to communicate in real time. However, because many of these options are not integrated into the familiar tools used in the daily work environment, they are not part of a cost-effective solution. The *SAP Collaboration Room* solution offers these real-time services through the portal and enhances the value of the information stored and accessed by sharing it in a contextual, ongoing team environment. Teams and individuals are provided with a tool set to enable them to collaborate more easily and efficiently.

Examples:

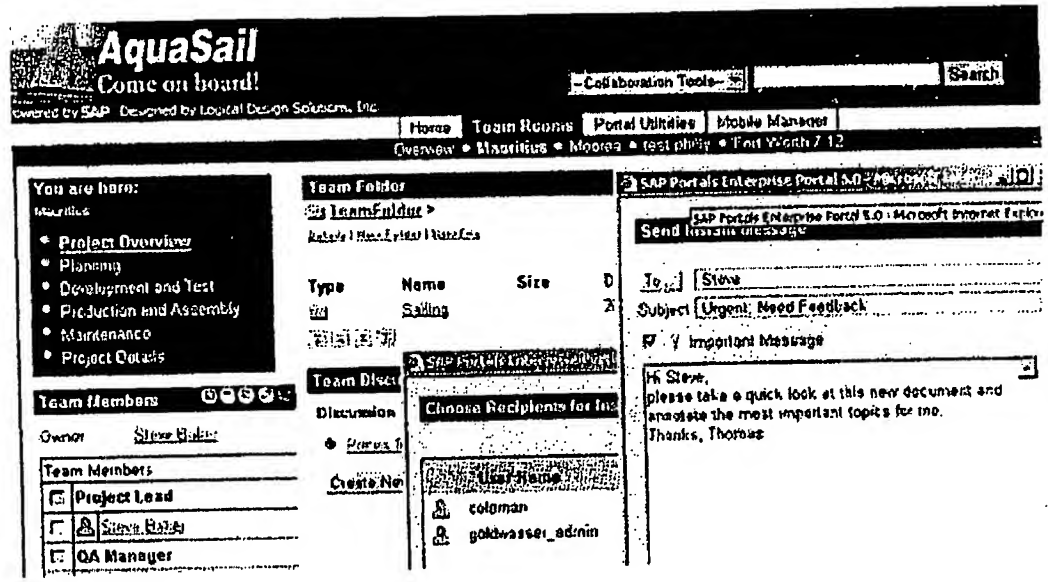
- Share iViews or applications from any portal page instantly

Legend

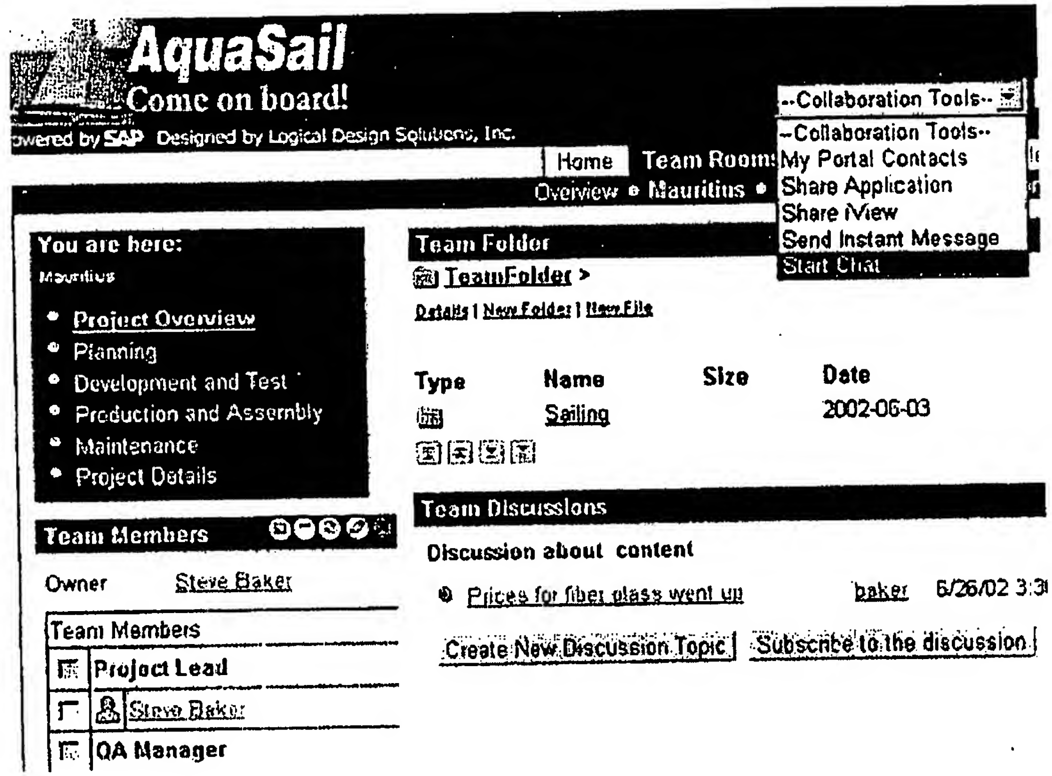
Book Document



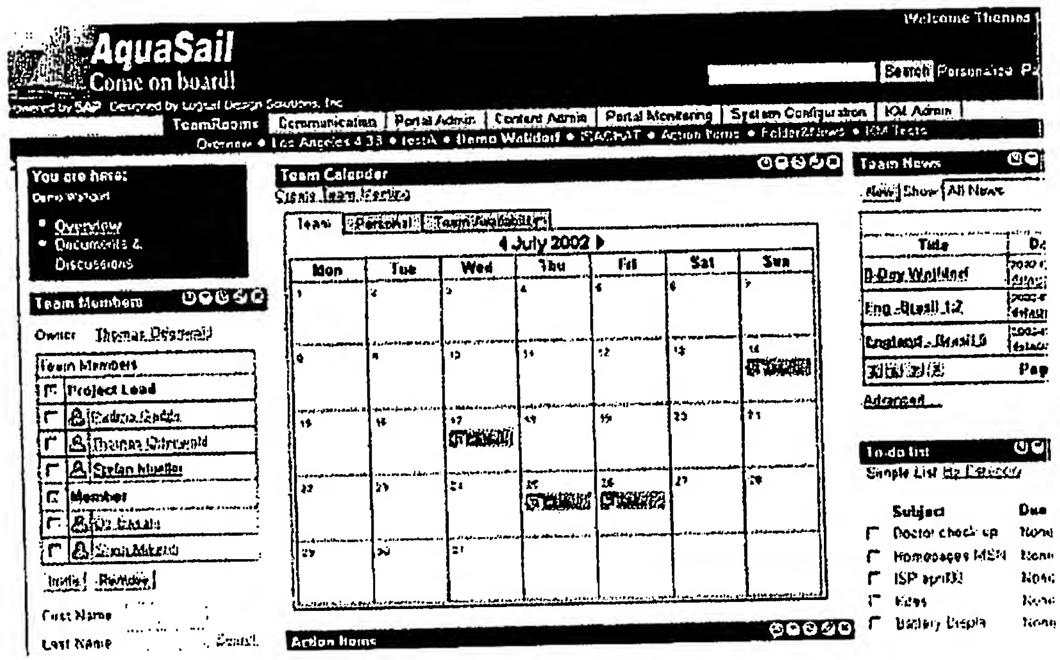
- Create instant message instantly from the portal by always knowing who is logged on to the portal and who is currently unavailable

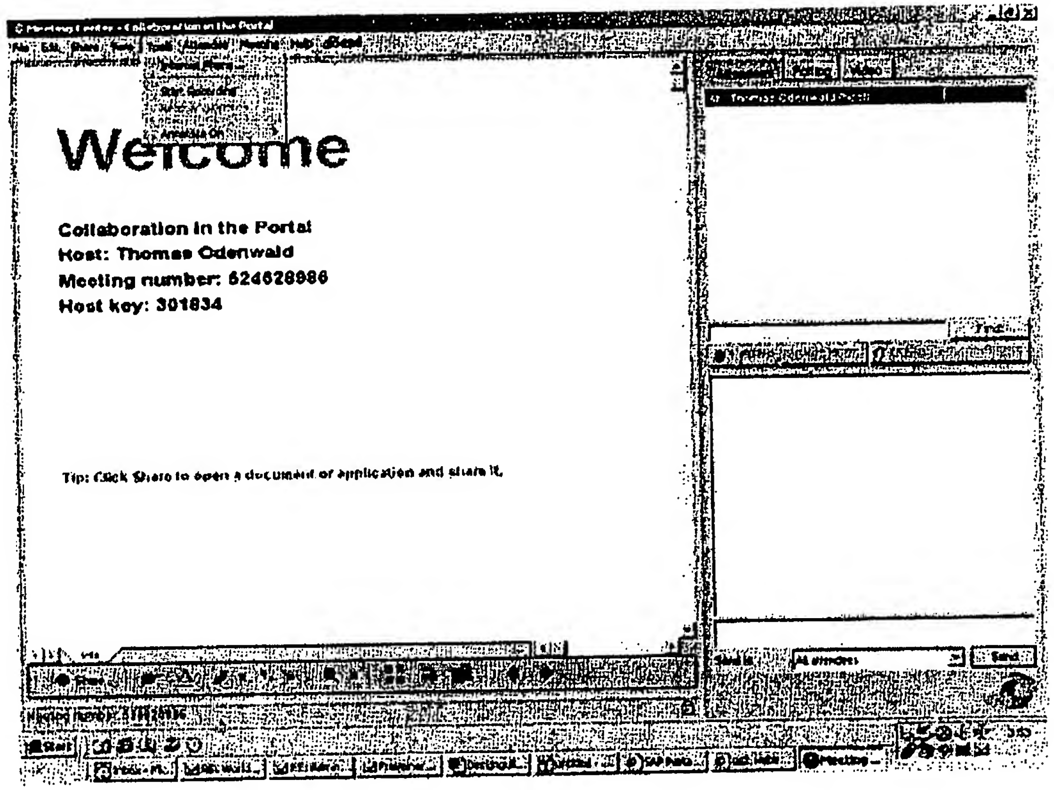


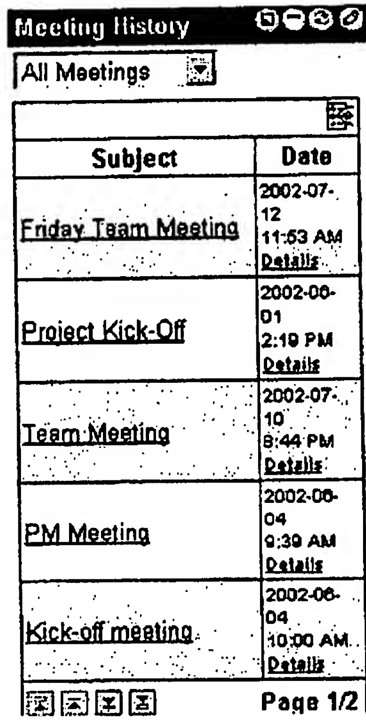
- Start public and private chats within the portal



- Schedule online team meeting, start meeting with mouse-click, and see the meeting results instantly in meeting history


AquaSail
Come on board!
Welcome Thomas
Search
Personalize
TeamRooms
Communication
Portal Admin
Content Admin
Portal Monitoring
System Configuration
KM Admin
You are here:
Overview
Documents & Discussions
Team Members
Owner Thomas Dressel
Project Lead
Member
First Name
Last Name
Team Calendar
Team
Personal
Team Availability
July 2002
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Action Items
Team News
Show All News
Title
Advanced
To-do list
Simple List
Subject
Due
Doctor check up
ISP
Battery Dispia


Welcome
Collaboration in the Portal
Host: Thomas Odenwald
Meeting number: 624628986
Host key: 301834
Tip: Click Share to open a document or application and share it.



In this scenario valuable meeting information can be captured seamlessly by attaching any file or link to the automatically generated meeting record. Any audio and video recordings included can also be started with a mouse-click. In a sense, these options allow you to build up your own e-learning center.

Examples:

1. Integration of Yahoo! broadcasting feature
2. Integration of WebEx Player

And this last example might just solve Bill's problems:

- All project related documents are always available in form of iViews
- All e-mails, calendars, and tasks are available in form of iViews
- Instant messaging buddy list is available
- Project/team-related and personal calendar is unified and available

Value Proposition?

Success depends on collaborative teamwork — and real-time services meet the challenges of a distributed work force. With teams no longer based in a single location, collaboration cannot happen exclusively in face-to-face meetings or in coffee corners.

Companies are already saving millions of dollars by using real-time services. The result is a reduced information exchange time, with

- single point of access to relevant information
- closer collaboration
- easier knowledge sharing
- reduced travel and reduced travel costs

Summary

Real-time services on the portal can be used as an extension to the *SAP Collaboration Room* solution or as a stand-alone solution. Real-time collaboration enables collaboration between individuals and teams, and manages the content they create. Rather than replacing existing tools, it integrates and unifies existing solutions in the portal environment.

Information stored in different places is available through one point of access. Users know exactly where they should be storing, sharing, and collaborating on documents and can meet and exchange information in a real-time environment.

top

print version of the article

"NetMeeting101,"
http://www.meetingbywire.com/NetMeeting101.htmz

NetMeeting 101

Home
Site Map
NetMeeting 101
NetMeeting 102
NetMeeting List
MSN Messenger
H.323 Corner
XP Messenger
XP/NetMeeting
Tips and Stuff
NetMeeting 3.0
Gateways
Contact Center
Consulting
Search
NetMeeting Store

What is NetMeeting?

NetMeeting is a real-time communications tool from Microsoft that allows individuals to communicate in pairs or groups over the internet or intranet (an IP enabled LAN) using audio, video and data communication.

Why is NetMeeting different?

NetMeeting has a number of characteristics that make it better than other similar tools:

- it is free (downloadable at Microsoft - Win2000 and XP versions are preinstalled and will not allow installation of downloadable versions)
- it is standards based (which means that it can communicate with other standards based products)
- it operates with 2 or more individuals in a meeting
- it has built in audio, video, whiteboard, chat, file transfer, program sharing and collaboration functions

What is required to run NetMeeting?

- Windows 95/98, Me, NT, 2000 or XP
- Internet or Intranet connection (TCP/IP)
- A sound card with a microphone and speakers (or better yet a headset with integrated microphone) is desirable

What is not required to run NetMeeting?

- NetMeeting 3.0 requires IE4.01+ to be on the system -- though there is no requirement to use it as your default browser
- NetMeeting does not require a video camera to view callers (to send video a camera is required -- parallel port or USB cameras are the easiest to install but capture card based cameras work best - a review of cameras and guide to selection is on the hardware page)

Click here to print this page

Add this page to your favorites!

Send this page to a friend

What are directory or ILS servers?

Most users of the internet are on dial up lines - not connected all the time. Each time they connect their IP addresses change (the IP address is at the heart of the internet -- all location information ultimately gets translated to IP address and computers intercommunicate using that as an address).

In order for potential calling computers to connect to you, they must have two pieces of information:

- they must know that you are online or connected
- they must know your current IP address

The ILS servers supply the function of providing this information. When you "Log on" to an ILS server you are telling the ILS server that you (identified by your supplied email address) are

connected to the internet, that you are at a certain IP address (a current bug in NetMeeting actually records the incorrect IP address if you are on an IP enabled LAN but connected through a dial up line) and that you are running NetMeeting and able to field calls. Now potential callers need know only two fixed pieces of information to call you:

- the ILS server that you are logged into or would log into if you are online
- the supplied email address

The ILS server you choose to use need bear no relationship geographically to where you are -- all that is necessary is that your potential callers know which you will log in to.

The ILS server knows whether or not you are online and if you are what your current IP address is. You can "log in" to an ILS server without appearing in the viewable directory so that only associates that know the ILS server and email address you supplied can find you.

Changed January 2,2003

I can't log on to a server!

There could be a number of reasons for this problem:

- you have an AOL installation that installed a 16 bit Winsock -- if this is the case you cannot log on to any server
- you are behind a proxy server that is not allowing your connections to the ILS server
- you have just logged out and the logout is not yet completed
- somebody else is logged on using your chosen email address -- this might be especially true if you use a common pseudonym email address
- the server you want to user is busy or overloaded
- apparently Win2000 somehow dictates a different LDAP port number -- it is necessary to add the port number(389) to the ILS name (i.e. ils.xxx.com:389)

Changed April 1,2000

Microsoft has outlined many of these issues in the support database

I get logged out every few minutes!

It seems that NetMeeting, when used on a dial up line, depends on the ICMP protocol (the same one that is used by ping and traceroute programs) to assure a connection before it does its regular update to the ILS server (every 2 minutes apparently).

If your router, your ISP, the ISP providing the ILS server or someone between is blocking or dropping ICMP packets (this is common in busy internet situations -- the "non-essential" ICMP packets are the first to be dropped by busy routers) you may be logged out.

Changed February 28,1999

Microsoft has published a support article on this issue.

What happened to the Microsoft ILS Servers and Internet Directory?

On December 15,1999 Microsoft decided to withdraw all ILS servers that it was running and let 3rd party servers handle the load and instead concentrate on MSN Messenger as vehicle for initiating NetMeeting calls.

No support for ILS servers was changed in NetMeeting so if you wish to continue to use an ILS

server you should pick one of the 3rd party servers available. Use NetMeeting HQ to find servers.

Changed December 27,1999

Finding an ILS server

Since Microsoft closed their servers it has become difficult for many people to find usable servers.

A number of websites I have noticed are maintaining ILS server scanners -- allowing you to determine current state of servers and to search a number servers at once.

Changed April 30,2003

Check out the sites -- NetMeeting Headquarters and VideoFrog, NetMeetingserver.net

I am not listed what is the problem?

There are a number of reasons why you might not see yourself listed:

1. You are not logged in to an ILS server (logging in can happen automatically on NetMeeting start up or on command depending on your preferences set up)
2. You have indicated in options that you want your listing not to be visible (this is like an unlisted telephone number -- people can still call you but they must know your number)
3. You are looking at a different ILS than the one you logged into.
4. You are looking at different category of user than the category you indicated on your login.
5. The ILS is overloaded or has failed
6. You have not refreshed the list to the most current available.

Changed June 9,2000

Why do I never get calls or why can't people who try to call reach me?

NetMeeting ILS registration works by registering your current IP address in the ILS system. People can call you through the ILS only if the address registered in the ILS is correct and reachable.

Various circumstances cause this not to be true:

- You are running on a TCP/IP enabled LAN and use a dial up ISP.
- You are running a TCP/IP enabled LAN and go through a proxy, firewall or NAT translator.
- You are running a TCP/IP enabled LAN and also use an Ethernet card that connects to a cable modem.
- You have WebTV software installed

This problem was prevalent with V2.x. Fortunately in V3.0 this is no longer a problem - NetMeeting uses the IP address of the adaptor that it will be talking to the ILS on as the IP to register - so most of the previous aberrant behaviour has been removed.

Changed April 9,2002

Manage which IP you register in the ILS?

A suggestion from Cuseeme users (who apparently experience a similar problem) was that the IP used is the IP of the last installed adapter -- and that deinstallation of all adapters Ethernet and dial up) and reinstallation with the IP that you desired to be registered on the last installed adapter was a solution. If you try this make sure you record all the settings on the adapters

before you deinstall.

Changed February 16,1999

Another suggestion from a NetMeeting user is to deinstall NetMeeting, connect to the internet

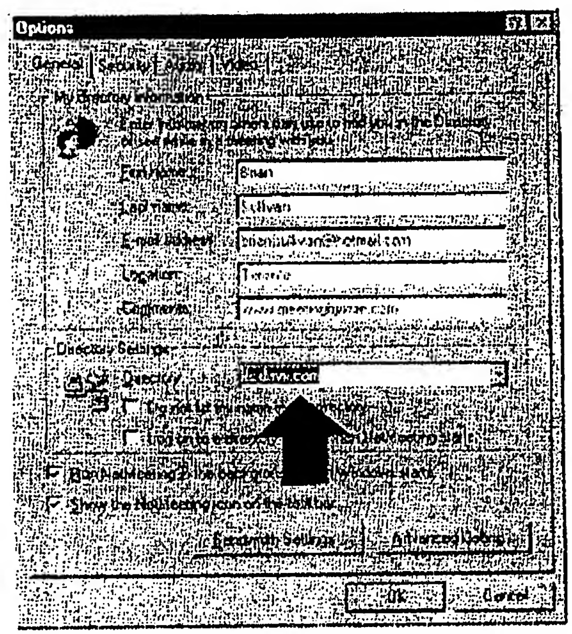
ILS theory vs. practice

Unfortunately the current ILS strategy is faulty and the overload problem mentioned above is becoming more and more common. In response to problems Microsoft has chosen to take all of its ILS servers permanently out of service and is favouring MSN Messenger as the prime connection strategy..

The ILS system itself seems unscalable and prone to breakdown or other faults. Nobody manages the system so a particular ILS server can go for days without functioning.

I have picked a new ILS server - how do I add it to the list?

To add an ILS server to the list of servers that you can log into or pick in the directory listing window click on the Server or Server name pulldown in the directory listing view or in the Tools/Options menu General tab (the server name text should now be selected) -- type the new name or paste the name in.



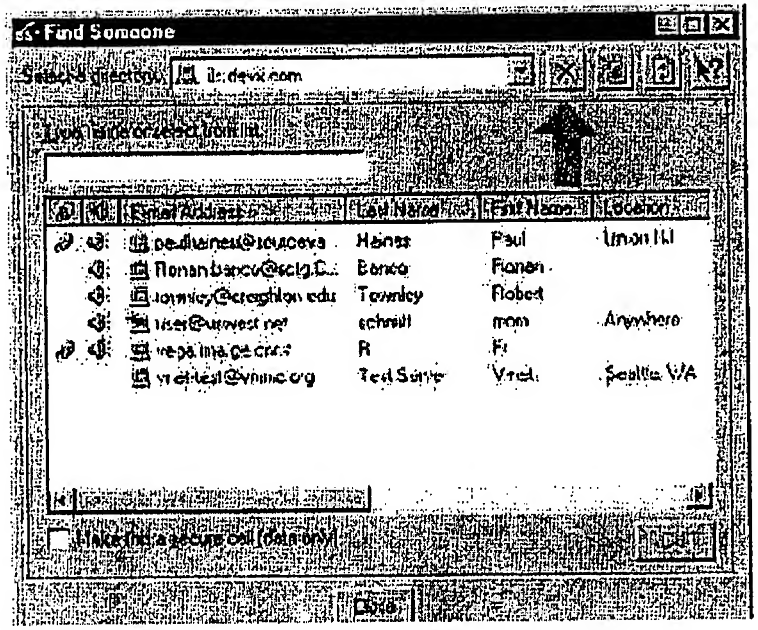
Changed July 22,1999

Can I delete

There is a limit of 15 servers allowed in the list. A function for deleting existing servers was

servers as well?

left out of the V 2.x of NetMeeting (to delete a server use the NetMeeting Super Enhancer program downloadable at the NetMeeting Place). To delete a server in 3.0 use Call menu. Directory item to display the "Find Someone" dialog. The current server can be deleted using the "X" button:



Added July 22,1999

Is there relief from this ILS dilemma?

There are a number of ways to avoid this ILS problem:

1. Find another less used more stable ILS server to register on. NetMeetingHQ and Videofrog , Chatpal also have ils server lists.
2. NetMeetingHQ and Videofrog have online ils scanners that provide web lists of ils servers. neetingserver.net has a similar service that is more family or work place friendly.
3. Use ICQ, AOL Instant Messenger or another buddy program as online signal and NetMeeting connection tool.
4. Use the TZO naming system , Dyndns or another dynamic naming service. This includes a permanent name that points your dynamic address.
5. Email partners informing them that you are online -- include your IP address (available by running ***winipcfg*** from the Start menu - run item for V2 and in the About box in V3) allowing them to call you directly.

6. Use Microsoft's MSN Messenger which has built in NetMeeting integration.

Changed April 30,2003

Making a Call using MSN/Windows Messenger

Since Microsoft closed all its ILS servers they have promoted Msn Messenger as the method for starting NetMeeting calls. Messenger is a much different mechanism than an ILS - though essentially it performs the same function as far as NetMeeting is concerned. It requires that you have a predetermined "buddy" list -- a list of individuals that have allowed you to determine their online status and to contact them.

Assuming you have downloaded and installed Msn Messenger and have established a list of buddies you can start a NetMeeting call from Msn Messenger using the "Start NetMeeting" menu item.

Unfortunately Microsoft in its infinite wisdom has chosen not to include this item in the XP "Windows Messenger" version. You can make it come back by setting the Messenger to Windows 2000 compatibility mode (right click on a Messenger shortcut, select properties, compatibility). For more information see the XP/NetMeeting page.

Changed January 02,2003

Can I avoid the ILS and the Internet and dial directly?

Versions of NetMeeting prior to V2.1 had a feature where you could make direct calls (modem to modem) avoiding the Internet and the ILS. This feature was removed in V2.1 and later.

It can still be done however. Noël Danjou has published information on how to to do this (a Word document) available from his download page.

I haven't tried the instructions myself the information but they seem complete and detailed.

Microsoft has published information as well.

Changed August26,1999

Can I set up NetMeeting to run on a LAN with no Internet access?

To set up a functional intranet to use NetMeeting:

All computers must have the TCP/IP protocol installed and bound to the Ethernet card and assigned TCP/IP addresses -- there are a number of ways to do this but the easiest is to assign an IP address from the non routable private set (I use 192.168.0.x with a mask of 255.255.255.0).

Disable Wins, and DNS unless machines have access to the internet or an internal DNS server. Install NetMeeting and set it up on all machines so that it: (all of these are in the Tools.. Options -- Calling tab) doesn't log on at start up.

Computers can now call each other in NetMeeting using the IP address 192.168.0.x as the address to call or computer name (identification tab of of Network properties).

There are other possible set-up strategies (IP addresses could be assigned by DHCP, you could run a DNS or WINS server to get computer name, you could run an internal ILS) but all add

extra complication.

Changed December 19,1999

Extensive LANs might require implementation of an ILS server to provide both presence and location information

Deleting the Most Recently used drop down list

The most recently used address drop down list (the black box above the video window) contains a list of the most recently typed in addresses to which completed calls where made.

It is stored in the registry at:
HKEY_CURRENT_USER\Software\Microsoft\Conferencing\UI\CallMRU

Deleting the key or contents will allow you to start the list anew -- I don't know the exact format of all entries but with some testing and manipulation you could probably add or remove individual items as well.

Added May 24,2001

Creating a Speedial list

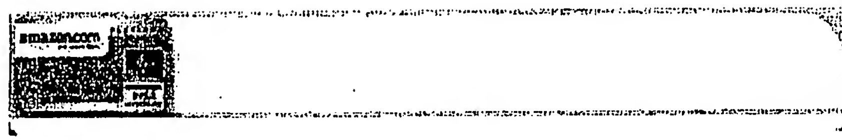
Creating a series of .cnf files in the "speeddial" sub directory of the NetMeeting install directory will create an address book the can be reused and transferred to other machines. The directory is accessible via the Call -> Directory pane drop down list.

Added May 24,2001

Test your audio video setup

Intel it seems is providing a test site to test your H.323 calling program (I think their own but it seems to work for NetMeeting.

Added January 02,2003


amazon.com

"NetMeeting102,"
http://www.meetingbywire.com/NetMeeting102.htm

NetMeeting 102

Home
Site Map
NetMeeting 101
NetMeeting 102
NetMeeting List
MSN Messenger
H.323 Corner
XP Messenger
XP/NetMeeting
Tips and Stuff
NetMeeting 3.0
Gateways
Contact Center
Consulting
Search
NetMeeting Store

Click here to print this page

Add this page to your favorites!

Send this page to a friend

This page has a large number of graphics and may take a long time to load. I apologize but I think most of the information is best expressed with pictures - I hope it is worth the wait.

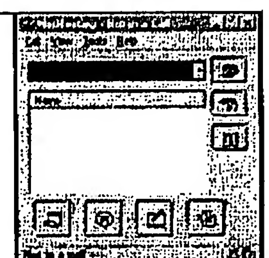
NetMeeting can be a useful tool but it can also be very frustrating. I have found that people sometimes get into difficulty after playing with various options and can't easily find their way to fix them. They end up with a program that is configured for some use that they never intended and can't make the kind of calls they want.

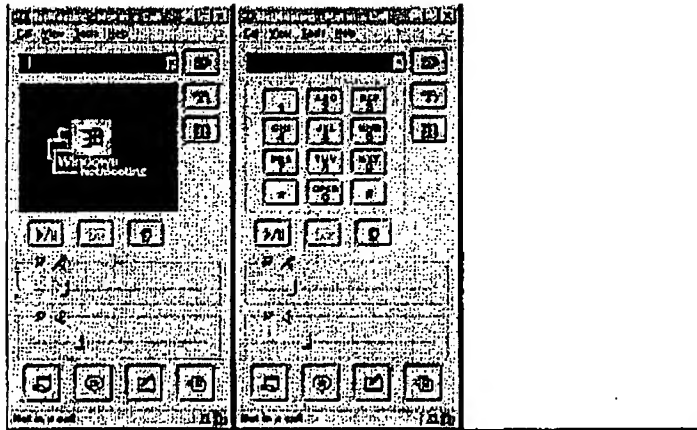
This page will list the most common problems I see with comments and solutions.

- Incorrect View Selection (no video)
- Incorrect Security Settings (no audio/video) - your settings incorrect
- Incorrect Security Settings (no audio/video) - the other party's settings incorrect
- Gateway Configured but not Required
- Hosting a Meeting not Required
- Incoming Audio but No Video (incoming video paused)
- Incoming Audio No Video (other end does not have video capability or has video paused)
- Audio Problems
- IEEE1394 (Firewire) cards and NetMeeting

Incorrect View Selection (no video)

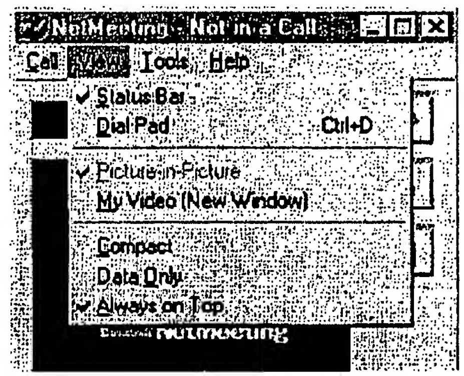
If your view of NetMeeting when you start up is not correct for video calls (no video window visible):





Correct	Incorrect	Incorrect

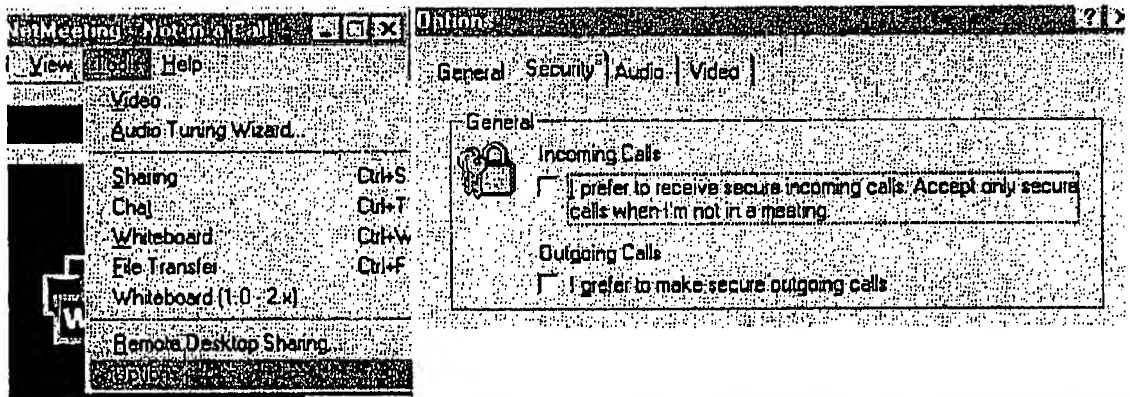
You have set your view so that you have no video window - this is a valid setting for some situations (using data only or use with a NetMeeting to telephone gateway) but for most people wanting to make audio/video calls these settings are incorrect.



To fix this problem make sure that the ***View*** menu does not have either ***Dial Pad*** or ***Data Only*** selected.

Incorrect Security Settings (no audio/video) - your settings incorrect

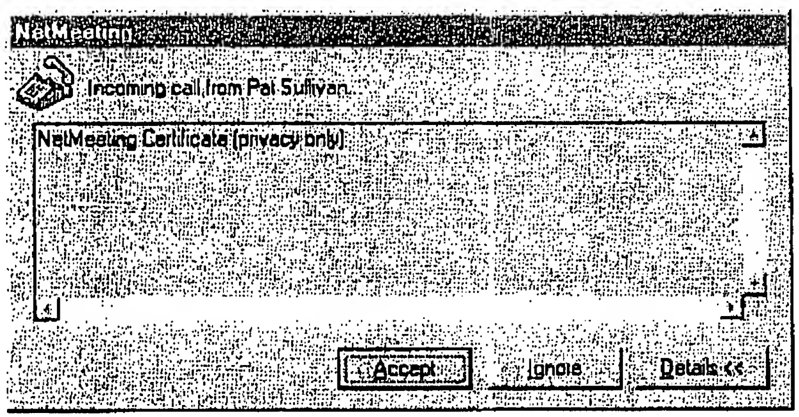
If you cannot connect to another party in an audio video call it may be because you or the other party have security settings that allow data only calls. In the ***Tools*** menu, ***Options*** item ***Security*** tab:



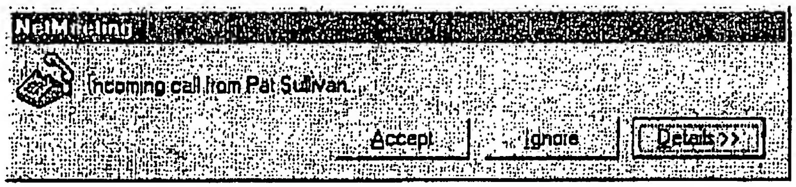
Make sure that the settings in the ***Security*** section about requiring ***Incoming Calls*** and ***Outgoing Calls*** to be secure are unchecked - making or receiving a "secure" call implies that it will be a data only call.

Incorrect Security Settings (no audio/video) - the other party's settings incorrect

If you receive an incoming call with a notice that looks like this:

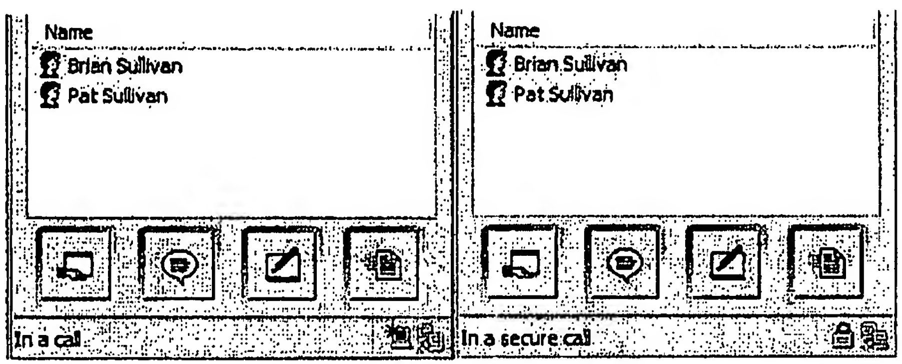


or this:



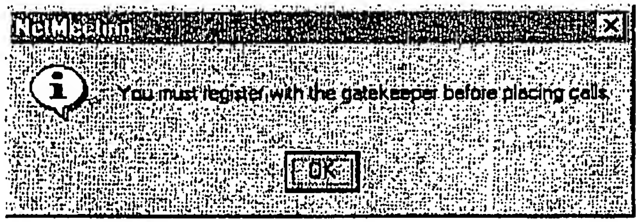
the other party has made a secure call which will be data only. This is what a normal incoming call looks like:

The two captures that follow show the difference between a secure call and a normal call in progress (notice the status bar at the bottom of the window).

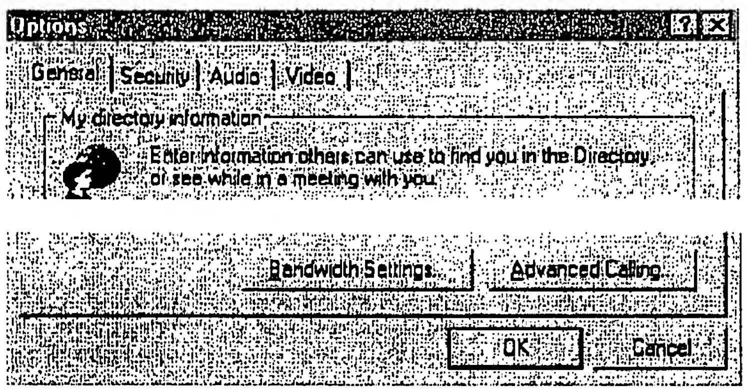


Gateway Configured but not Required

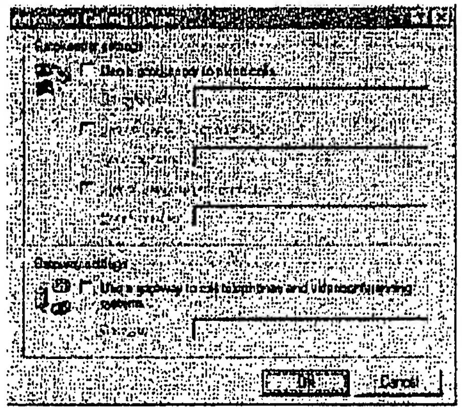
If you try make a call and get a message like:



Likely you have configured the ***Advanced Calling*** features incorrectly in the ***Tools*** menu ***Options*** item - ***General*** tab

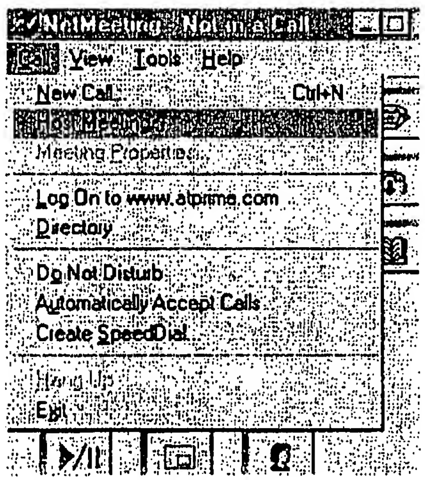


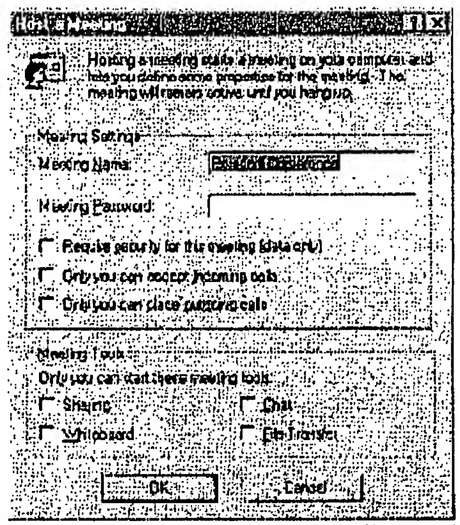
Clicking on the ***Advanced Calling*** shows dialog box like::



All items in this menu should be unchecked (as in the graphic) for normal operation.

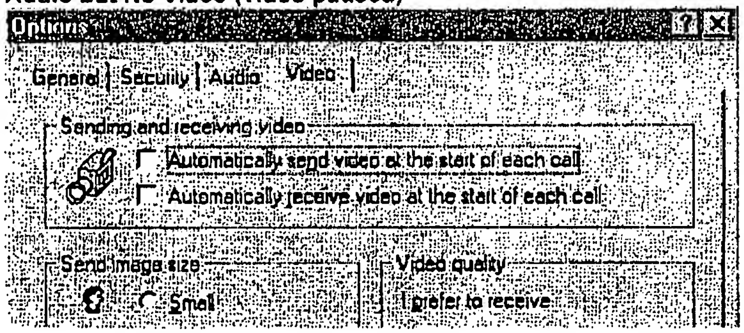
Hosting a Meeting not Required





Under normal circumstances the host meeting function is not required: All items in this dialog should be unchecked:

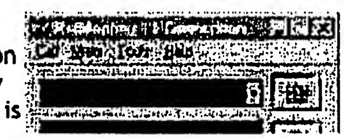
Audio but No Video (video paused)



If your video setting in the ***Tools*** menu, ***Options*** item, ***Video*** tab is set to not automatically send or receive video when you start a call (a setting I recommend because it sometimes help establish the call faster), it will be necessary to manually start the incoming and outgoing video using the ***pause/play button*** at the lower left below the video window. Incoming and outgoing video can be paused or played independently by right clicking on the image (either the incoming image in the video window or your image in the picture-in-picture box or a detached "My Window") and checking or unchecking the ***Pause*** item.

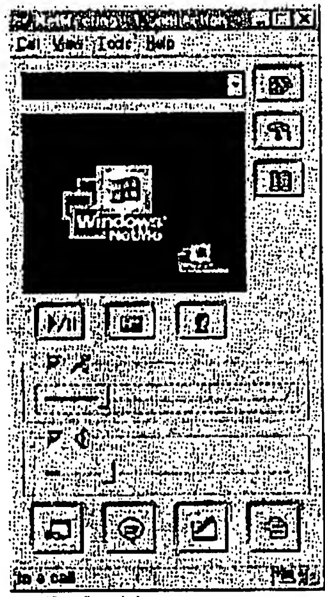
Incoming Audio No Incoming Video

If your settings are set to play incoming video and you are seeing nothing (but audio from the other party is heard) either the other party has no video camera or is not transmitting. You or they can pause the video incoming or outgoing by right clicking on the video and checking or unchecking the pause item.



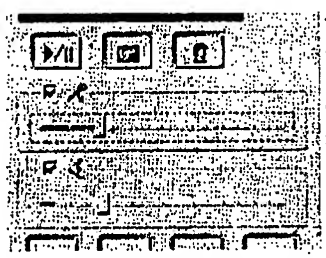
You can determine whether the other party apparently has audio or video capability by making sure that you are in ***View Participant List*** mode. Clicking on an individual and selecting ***Properties*** will show you what audio/video capability the party apparently has. It is possible the even though audio or video capability is

cannot effectively use it (i.e. they might have a TV card with no camera, a sound card but no mic)



If you instead have the audio meters view you can toggle between this view and the participant view using the button on the right below the video window.

Audio Problems



The audio meter view (available by clicking on the button on the bottom right of the video window if you are in the participant view) allows control of the audio properties of the call - the slider should be set at the lowest possible setting that will allow comfortable natural sound in both directions. The speaker section should have one green rectangle when the call is fully connected -- if it does not likely you are experiencing a problem with the H.323 connectivity caused by a router, firewall or proxy blockage (the Audio Tips page has a discussion) or the call was made as a data only call (see above).

If your microphone shows no meter movement when you speak likely either the microphone or its connection is faulty or your audio mixer is misconfigured (again the Audio Tips page has a discussion).

If the other party is experiencing echo of their voice and you are not using headphones (both you and the other end should be)-- it is possible to use your end in a half duplex mode by clicking off the microphone check box when you are speaking.

IEEE1394 Firewire cards and NetMeeting

IEEE1394(Firewire) cards (and DV cameras) do not usually provide the required drivers (with VFW interfaces) NetMeeting capture and thus cannot normally be used as video conferencing cameras.

At least one correspondent has found a (perhaps clumsy but usable) solution to the problem -- his comment is in response to my standard - it doesn't work response:

"Actually, this is not true. I have such a configuration and I have managed to use the camera with netmeeting, with help of a product named "SoftCam" from Luminosity Software (www.softcam.com), together with the "AMCAP.EXE" program, which is part of Microsoft's DirectShow SDK. Here's the setting: -amcap.exe runs in a corner of the screen and displays a real-time preview of the DV cam. It can be resized at will -When running Netmeeting, I choose the "SoftCam" video source. -In the SoftCam control panel, I select "live" mode, and make sure that the capture frame matches amcap's preview area.

As far as I can tell, it works as well as a "native" VfW device. The only thing is that you must remember not to clutter the capture area with another window. I agree that the setting is not very straightforward, and I would like to see a little piece of software that combines amcap and softcam into a single VfW driver that takes its source from any WDM video device. I don't see any technical problem in that, and I am surprised that it doesn't exist yet. Microsoft claims that it supplies a VfW-to-WDM mapper that is supposed to do exactly this, but it requires additional software from the hardware vendor."

Many individuals have used the Trackerpod software as a (clumsy but usable) work around -- it has a WDM (new style) to VFW (old style) capture interface translation.

Another correspondent indicates:

"It IS TRUE that DV cameras coming in over Firewire (or anything else) do not work because they typically do not come with the kind of drivers that Netmeeting uses.

It is NOT true that Firewire webcams do not work. I have four kinds of Firewire cards on which I can use video in all cases that I have tried. These are:

1) Audigy Firewire Interface
2) PCMCIA Firewire (for laptops)
3) Orange Micro Firewire (three ports)
4) Orange Micro Ethernet/Firewire combo board

I have an Orange Micro iBot camera and have successfully used it with all of these boards on both Windows 2000 and Windows XP. I have not been able to use it on Windows NT because drivers to not exist for firewire that will handle a camera (drivers DO exist for IP). I have not used any of this on the Windows 98 platform because I do not have sufficient CPU power (it's an IBM ThinkPad 240 with a celeron) to run the video, but I suspect it would if I had a system with enough gas.

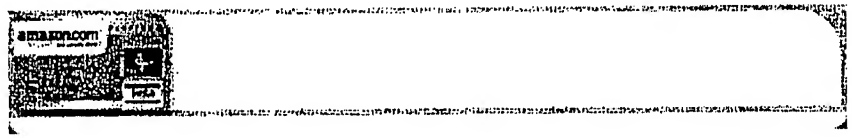
The advantages of the Firewire solution is that it can support a far higher data rate than USB 1.1. As USB 1.1 can do a

maximum of about 1mbps, it can not support a 30fps full color data rate. Thus, there is onboard circuitry on the camera does compression before sending the data over the wire to the host. The benefits of this are that the work of compressing the video data flow can be, in part, offloaded from the main system processor. That can be important with older systems.

The Firewire interface has a 400mbps data rate which will easily handle 30fps full color; no surprise as it was developed in part to handle DV camcorders. Since the host is getting the raw data, it can use more sophisticated methods to do compression which can also change as new drivers are introduced. Of course, you have to have sufficient CPU power to do this. I only run the Firewire iBot camera on either a 1.1 Ghz or a dual 900Mhz system.

I would recommend that you change the title to "DV Cameras and NetMeeting" as this would focus attention on the fact that is cameras without proper drivers. Firewire itself is simply the transport mechanism and doesn't have much to do with whether NetMeeting will actually work or not."

Problems, comments, questions: Email webmaster
Changed:Monday October 06, 2003 12:28 -0400



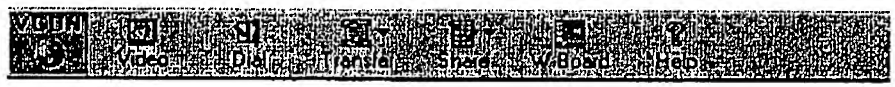
"Instructions on Application Sharing and Data Collaboration," VCON Escort and Cruiser,http://www.vide.gatech.edu/docs/share/

Instructions on Application Sharing and Data Collaboration

VCON Escort and Cruiser

Choosing the Data Collaboration Option

The VCON clients come with the capability of doing application sharing and data collaboration with either Microsoft's NetMeeting or with VCON's built in T.120 system. Therefore the first step in doing application sharing or data collaboration is to identify your choice. To do this, place your cursor on the Conference Panel (topmost gray bar.)



Press the right mouse and choose "Properties".

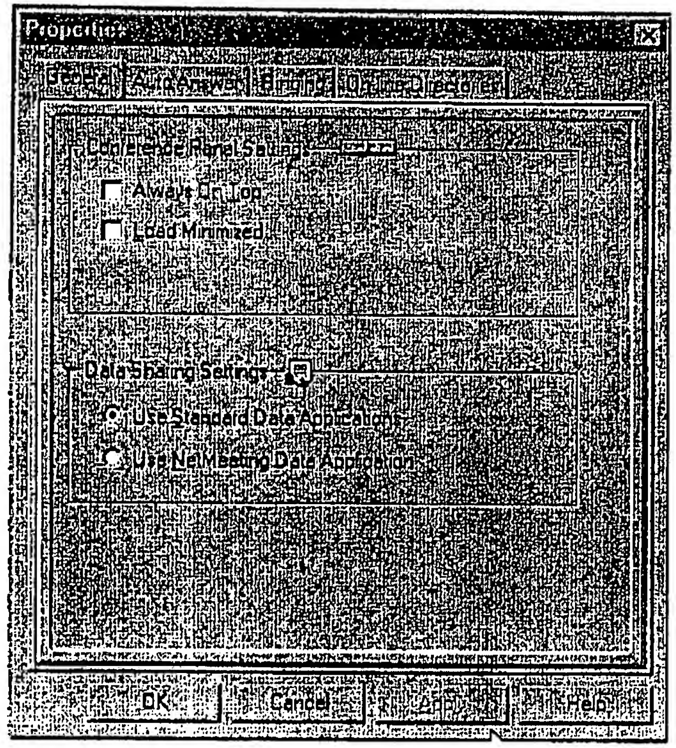
Here you will see several configuration options. You will find the "Data Sharing Settings" under the "General" tab. The VCON client gives you the option of using Microsoft's NetMeeting or it's own T.120 implementation which it calls the Standard Data Applications. Some testing and experience has shown several things:

- If the other client(s) in the call is(are) from another vendor, all clients should attempt to use NetMeeting.
- If only VCON clients are in the call, all should select the same Data Sharing Setting....either NetMeeting or the Standard Data Applications. Unpredictable cursor action/affect seems to result otherwise.

We will give examples of both in this document.

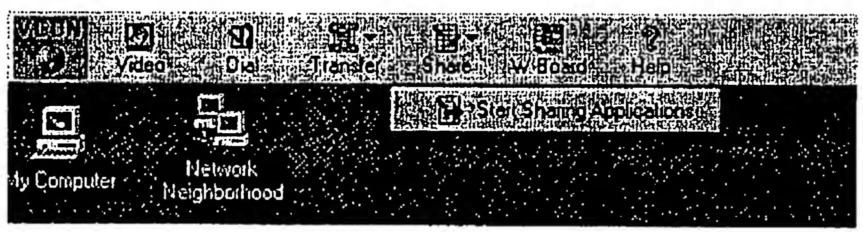
Data Sharing through the Standard Data Application

Click the "Use Standard Data Application" and then "OK". You will need to restart your client before the change actually takes effect.

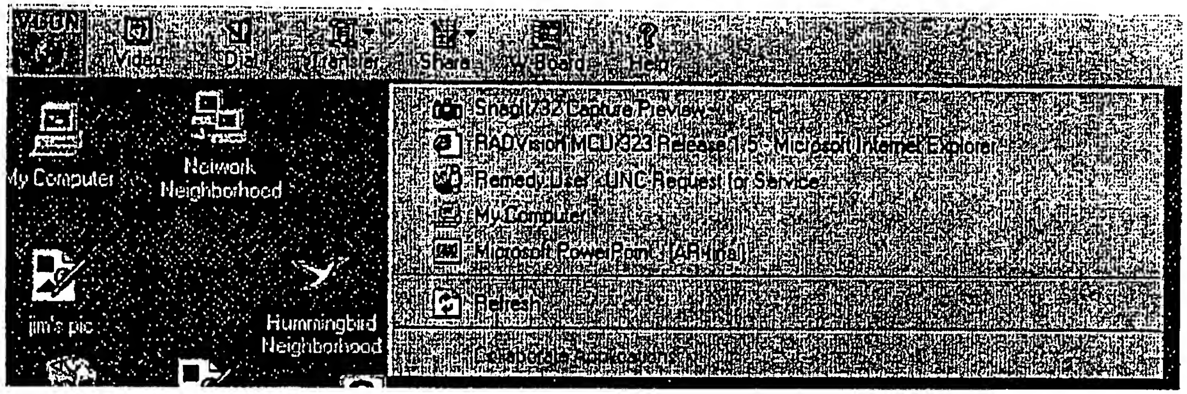


Establishing Application Sharing

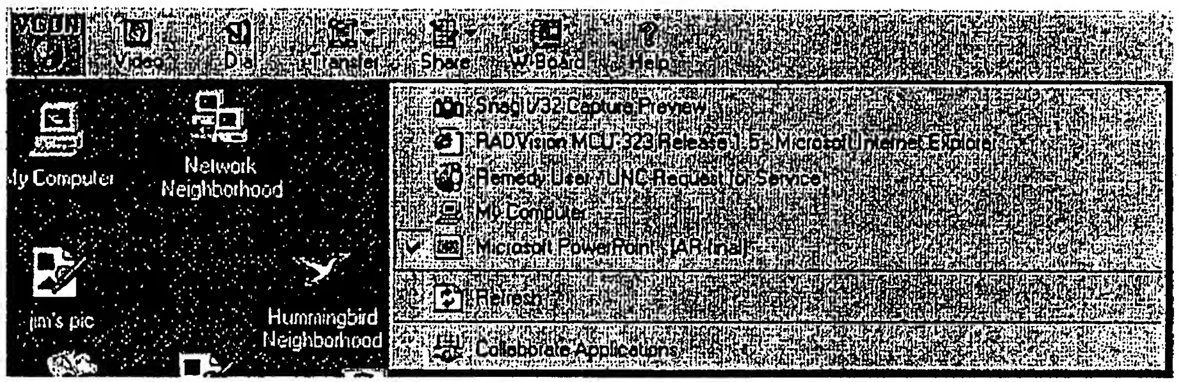
Either person can establish application sharing. We will call this person the "share-lead". The share-lead will go to the conference panel and click on "Share"



dragging down to highlight "Start Sharing Applications". Clicking on "Share" again will now show which applications are available for sharing.



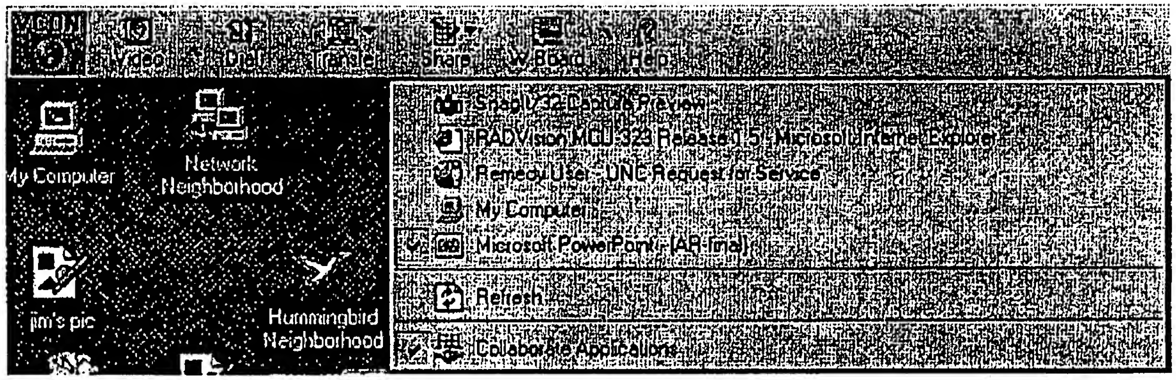
In this example, we will share a Power Point Presentation called "AR-final". To do his we drag down and highlight that entry. Clicking on "Share" again will now show



The Power Point application window and the open presentation will now appear on the other end station(s). The others will only be able to view the application and the share-lead's activities on it. (Note: If the share-lead puts any other, non-shared windows on top of the Power Point window, they will show on the other end station(s) as rather unsightly cross-hatched blocks of the same size as the unshared windows -- basically limiting or blocking their view of the Power Point.)

Establishing Data Collaboration

The share-lead can now allow the other end-station(s) to traverse through and modify the application by enabling the data collaboration mode. To do this, the share-lead will again click on "Share", this time dragging down and highlighting "Collaborate Applications".

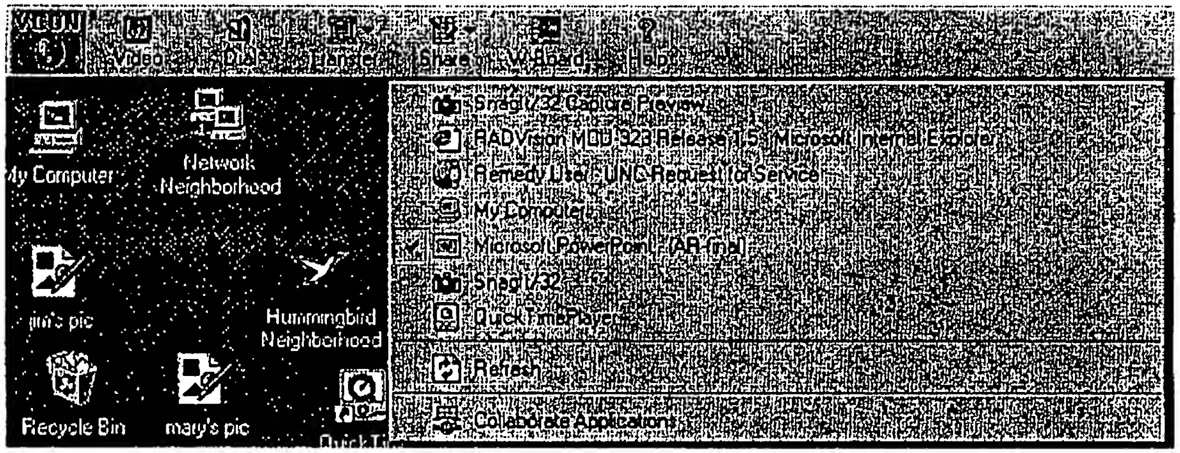


Now anyone in the conference can navigate through any shared documents, make changes to any shared documents, save or replace any shared documents, control the behavior of any shared applications. Several things should be mentioned:

- First, the application is actually running on the share-lead's machine. Any file activities will therefore happen on their machine as well. The other participants, for example, cannot save a shared document on their own machine. (See the "Transfer" button for moving files.)
- Secondly, for control of an application to transfer from one person to another, the new person can simply click their mouse anywhere in their screen. The cursor then falls under their control.
- And finally, while in data collaboration mode, there is only one cursor among all machines in the conference. It does not seem to matter whether someone is trying to use the shared application or a non-shared (private) application running on their machine. Should someone need to use the cursor (say to do a quick email check), proper protocol would seem to be "May I use the cursor for a minute" and, when finished, "Okay, someone else can use it." Unless such a protocol is followed, the collaboration could deteriorate into something we could term "Dueling Cursor" syndrome. We don't like it, we may report it. It doesn't seem to be a reasonable feature at this point - perhaps a configuration shortcoming and hopefully not a part of the standard.

Breaking the Collaboration or Sharing

To turn off data collaboration, simply click on "Share" and highlight it again. Notice that it is now unchecked.

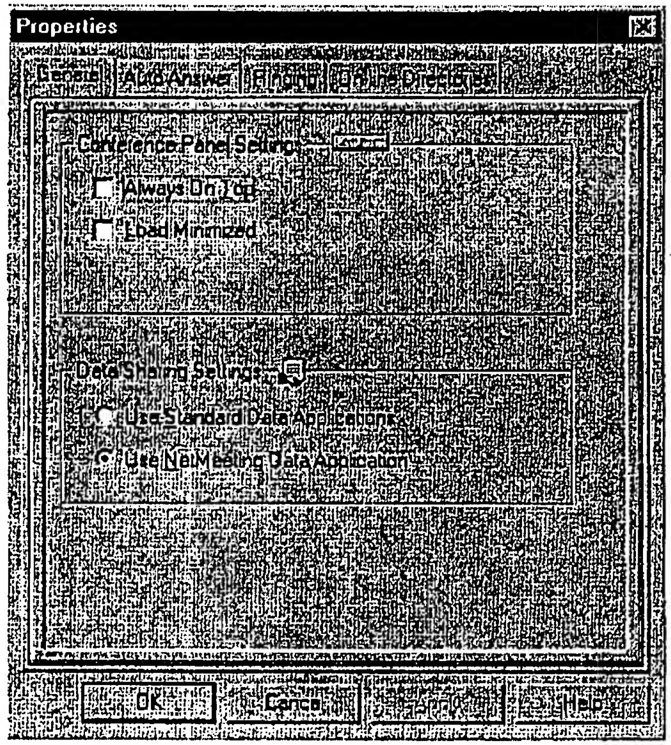


Application sharing is turned off similarly. Also notice that a new application has shown up on the list -- QuickTime Player. Anytime the share-lead starts up a new application, it will only appear under their "Share" button after they do a "Refresh" under this button.

At this point the participants can continue their conversation or hang up as usual.

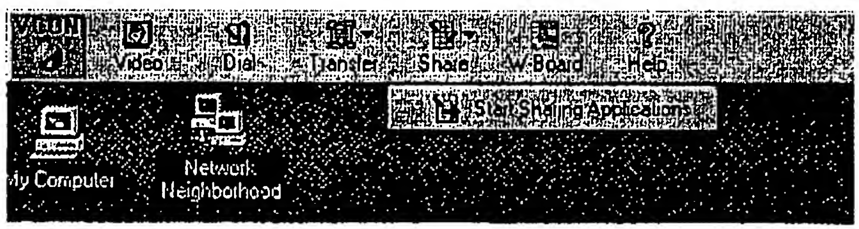
Data Sharing through NetMeeting

Click the "Use NetMeeting Data Application" and then "OK". You will need to restart your client before the change actually takes effect.



Establishing Application Sharing

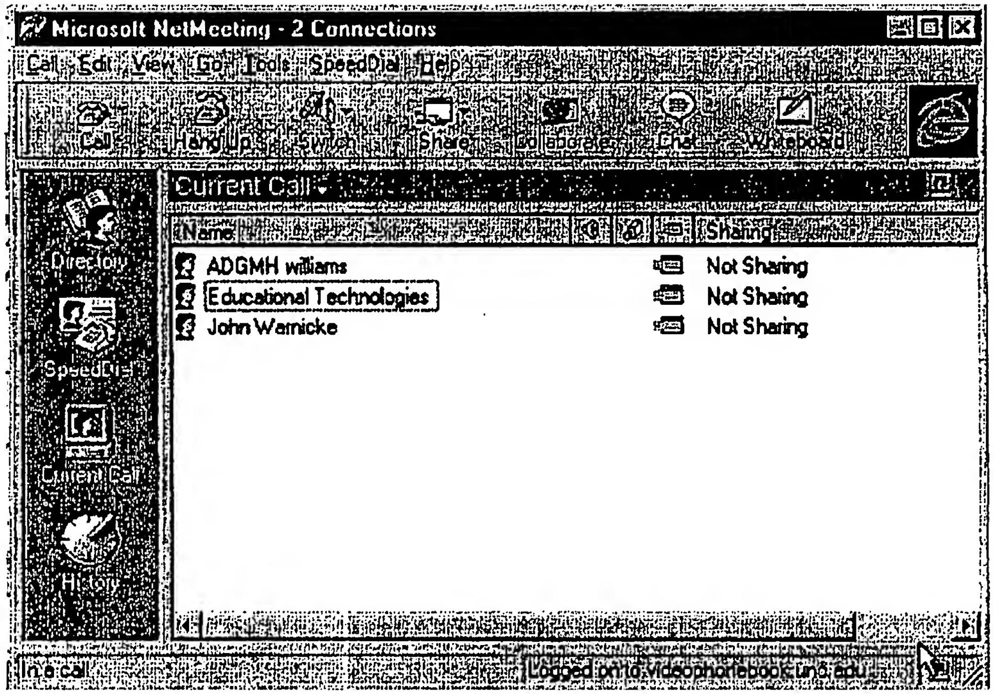
Either person can establish application sharing. We will, as above, call this person the "share-lead". The share-lead will go to the conference panel and click on "Share"



dragging down to highlight "Start Sharing Applications". This will cause NetMeeting to start on all workstations (meaning that it must be installed prior to the call.)

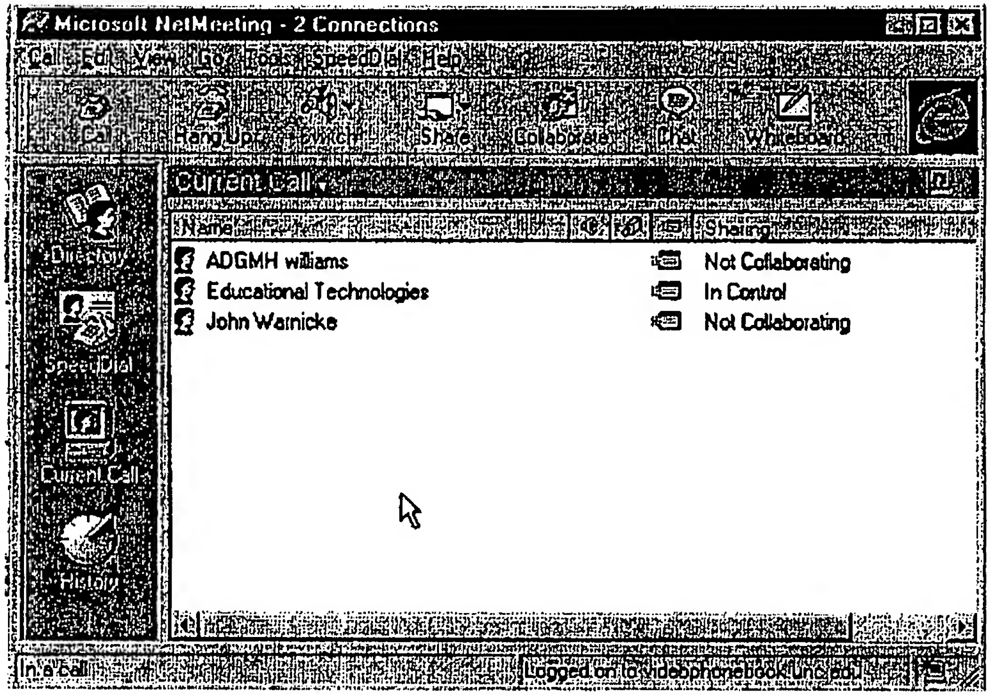
The NetMeeting Interface

At this point the video conferencing is happening through the VCON client and the application sharing and/or data collaboration is (or will soon be) occurring through NetMeeting. The NetMeeting window will initially appear as something like



At this point, no sharing or collaboration is taking place. The share-lead will start them by using the "Share" and "Collaborate" buttons on the NetMeeting window. Clicking on either will show which applications are available for sharing or collaborating. The share-lead will select any items they wish to share from this list.

Since the share-lead starts up the sharing and collaboration in this example, they are shown as "in control" initially (here it is Educational Technologies, ET for short.)



While in sharing mode, John and Williams will be able to see what ET has shared with them. If ET chooses to collaborate the application, John or Williams can take control of the application simply by clicking in the application window. For example, if John takes control of the application, the NetMeeting window would then change to show ET "Collaborating", John "In Control", and Williams "Not Collaborating". Williams can take control by clicking on the application window whenever his time comes to contribute information or operate the application.

As mentioned above for the Standard Data Applications, now anyone in the conference can navigate through any shared documents, make changes to any shared documents, save or replace any shared documents, control the behavior of any shared applications. Several things will be mentioned here as well:

- First, the application is actually running on the share-lead's machine. Any file activities will therefore happen on their machine as well. The other participants, for example, cannot save a shared document on their own machine. (See the "Transfer" button for moving files.)
- Secondly, for control of an application to transfer from one person to another, the new person can simply click their mouse anywhere in their screen. The cursor then falls under their control.
- And finally, while in data collaboration mode, there is only one cursor among all machines in the conference. It does not seem to matter whether someone is trying to use the shared application or a non-shared (private) application running on their machine. Should someone need to use the cursor (say to do a quick email check), proper protocol would seem to be "May I use the cursor for a minute" and, when finished, "Okay, someone else can use it." Unless such a protocol is followed, the collaboration could deteriorate into something we could term "Dueling Cursor" syndrome. We don't like it, we may report it. It doesn't seem to be a reasonable feature at this point - perhaps a configuration shortcoming and hopefully not a part of the standard.

Breaking the Collaboration or Sharing

Click on the Share or Collaborate button. Which items are actively being shared or collaborated are shown by the display of a checkmark to the left of those applications. The person who originated the sharing or collaboration can simply select any application (again) to toggle it off.

At this point the participants can continue their conversation or hang up as usual.

"Instructions on Multipoint Application Sharing and Data Collaboration," VCON Escort and Cruiser with the RadVision MCU,http://www.vide.gatech.edu/docs/multi-share/

Instructions on Multipoint Application Sharing and Data Collaboration

VCON Escort and Cruiser with the RadVision MCU

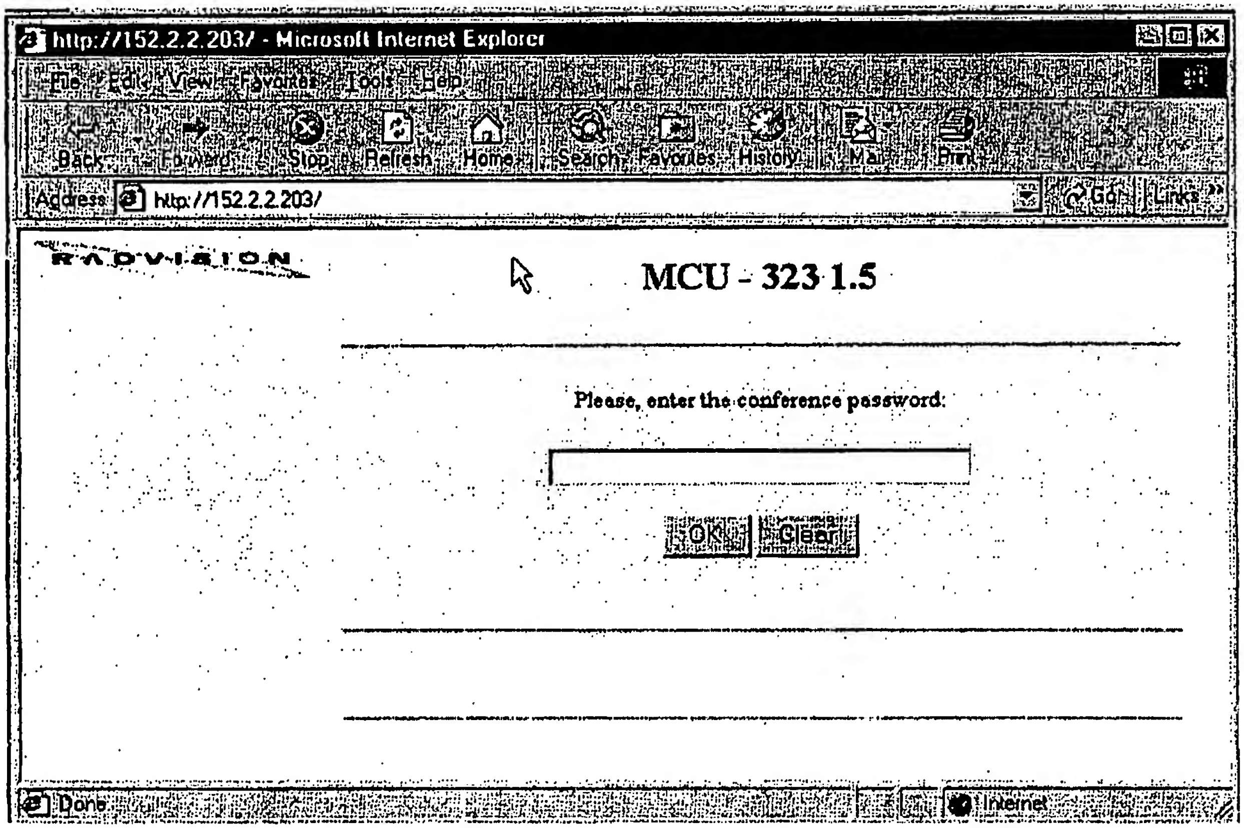
General application sharing and data collaboration instructions can be found in Instructions on Application Sharing and Data Collaboration. This material includes some additional information on what is required to start application sharing and data collaboration when in a multi-point call under a RadVision MCU and Gatekeeper.

Establishing the Data Share Group

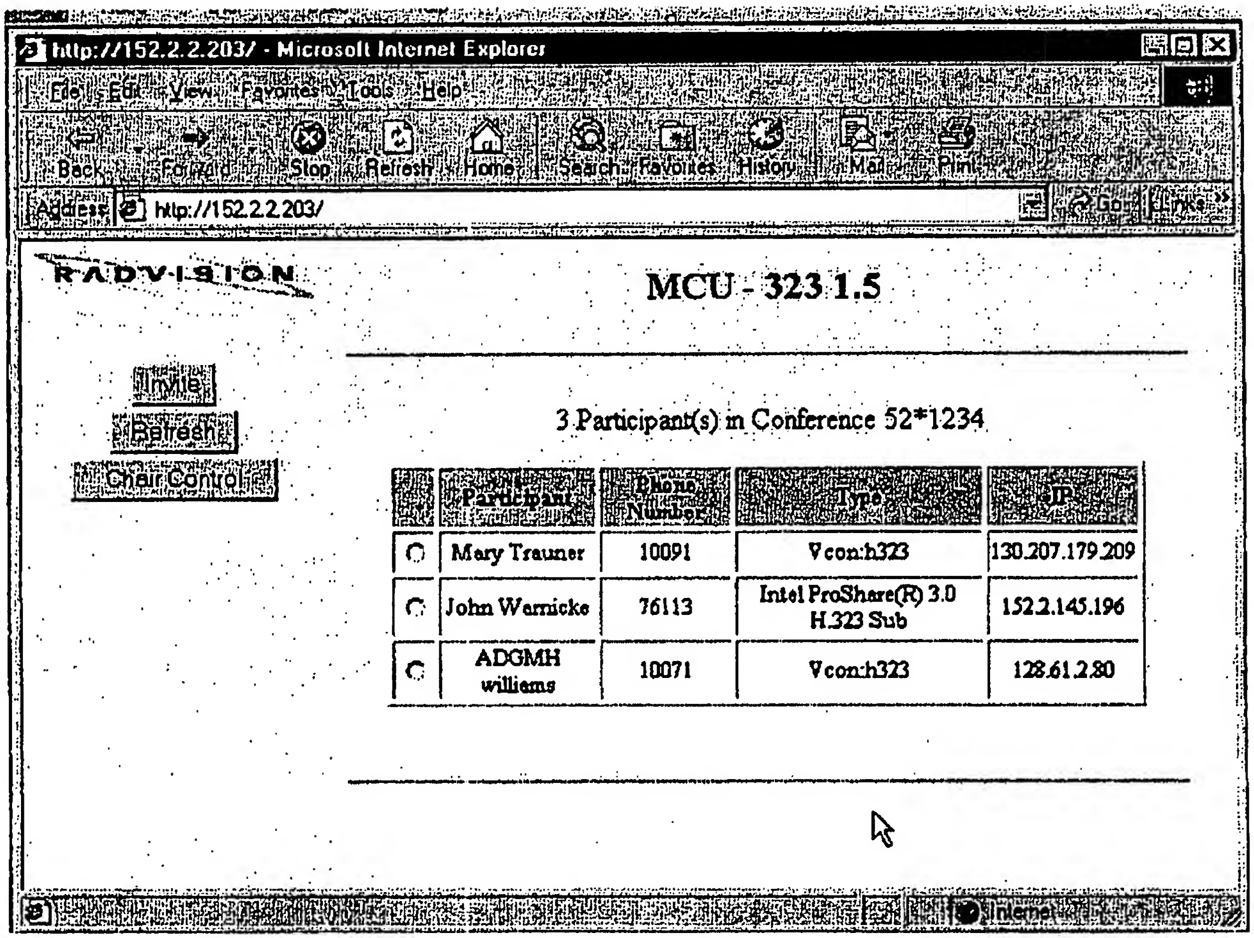
Since there will be three or more people in a multi-point conference, one person needs to bring all others into the MCU "Data Share" mode. (We'll call this person the share-lead.) To do this, the share-lead should start the Internet Explorer browser. (The interface does not work properly with Netscape; this *restriction* is being reported to RadVision.) The share-lead should then link to their MCU via its ip number. For this example

http://152.2.2.203

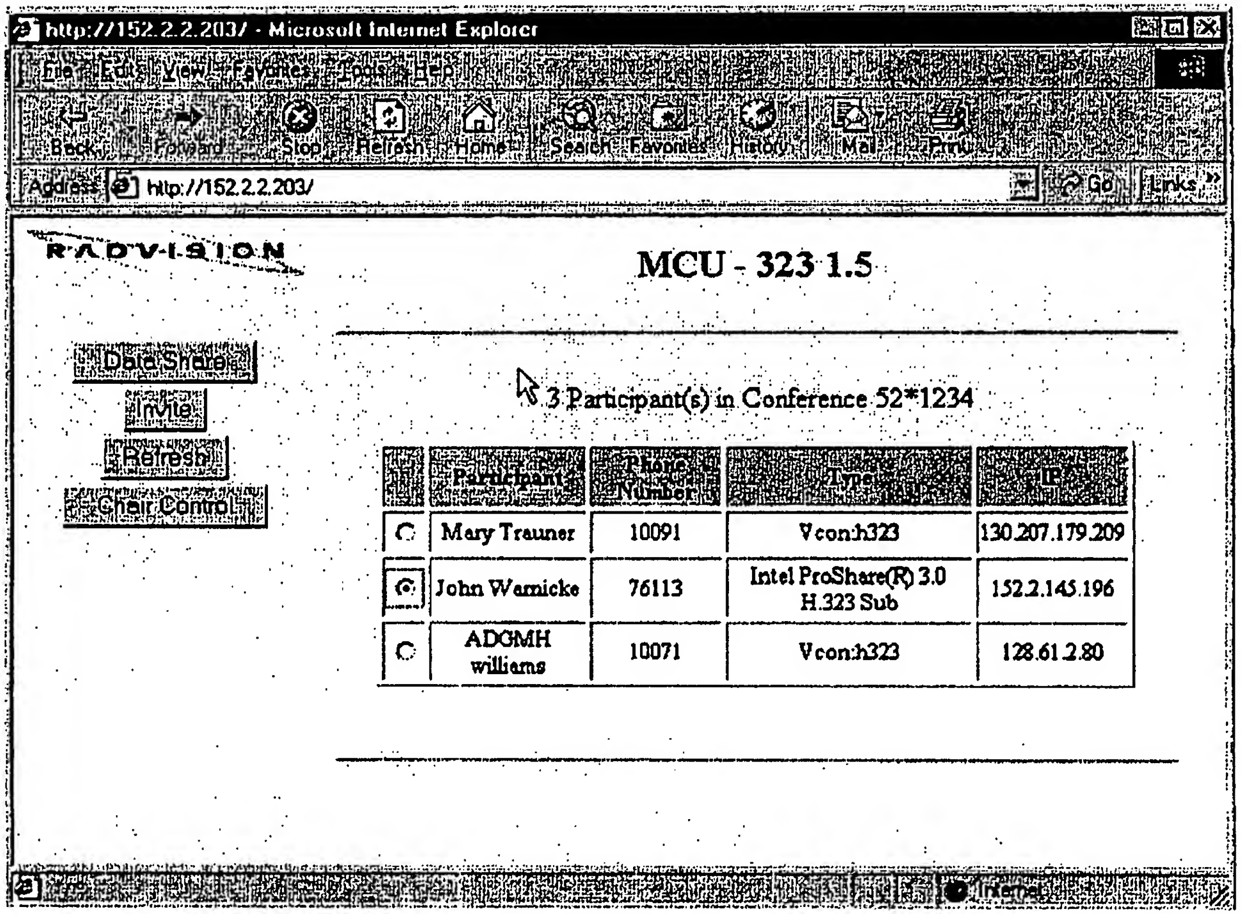
The MCU window will come up asking for a conference password.



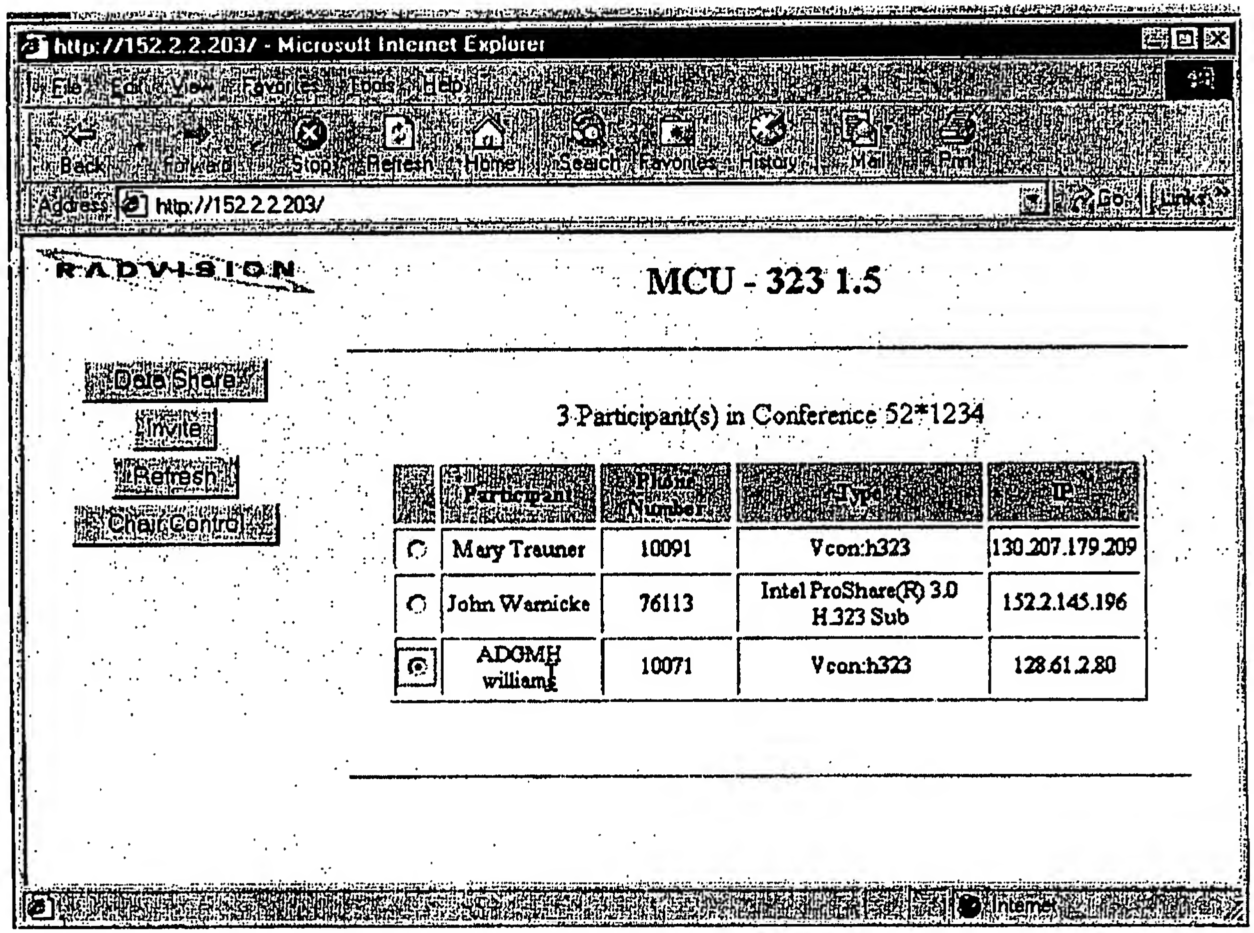
Enter that password (typically this is the same number that you dialed to reach the MCU) and click "OK". The window will show who is currently in the multipoint conference. (Note: This is not dynamic, therefore "Refresh" should be clicked every so often to see if anyone else has joined in or left.)



Each person currently in the conference is listed; a radio box appears to the left of each name. Let's say that Mary is the share-lead in this example. For each person with whom she wants to application share or data collaborate, she will click the radio box and then click "Data Share". First she will include John.



Then she will add in Williams.



If they are on VCON clients using the Standard Data Sharing, the VCON "Share" button scenario will be used. If NetMeeting is their application sharing choice, a NetMeeting window will appear on each screen as they are added to the Data Share. See Instructions on Application Sharing and Data Collaboration for further details on choosing applications and enabling sharing and/or collaboration under either of these options.

"Instructions on Multipoint Application Sharing and Data Collaboration," VCON Escort and Cruiser with the RadVision MCU,http://www.vide.gatech.edu/docs/multi-share/

Instructions on Multipoint Application Sharing and Data Collaboration

VCON Escort and Cruiser with the RadVision MCU

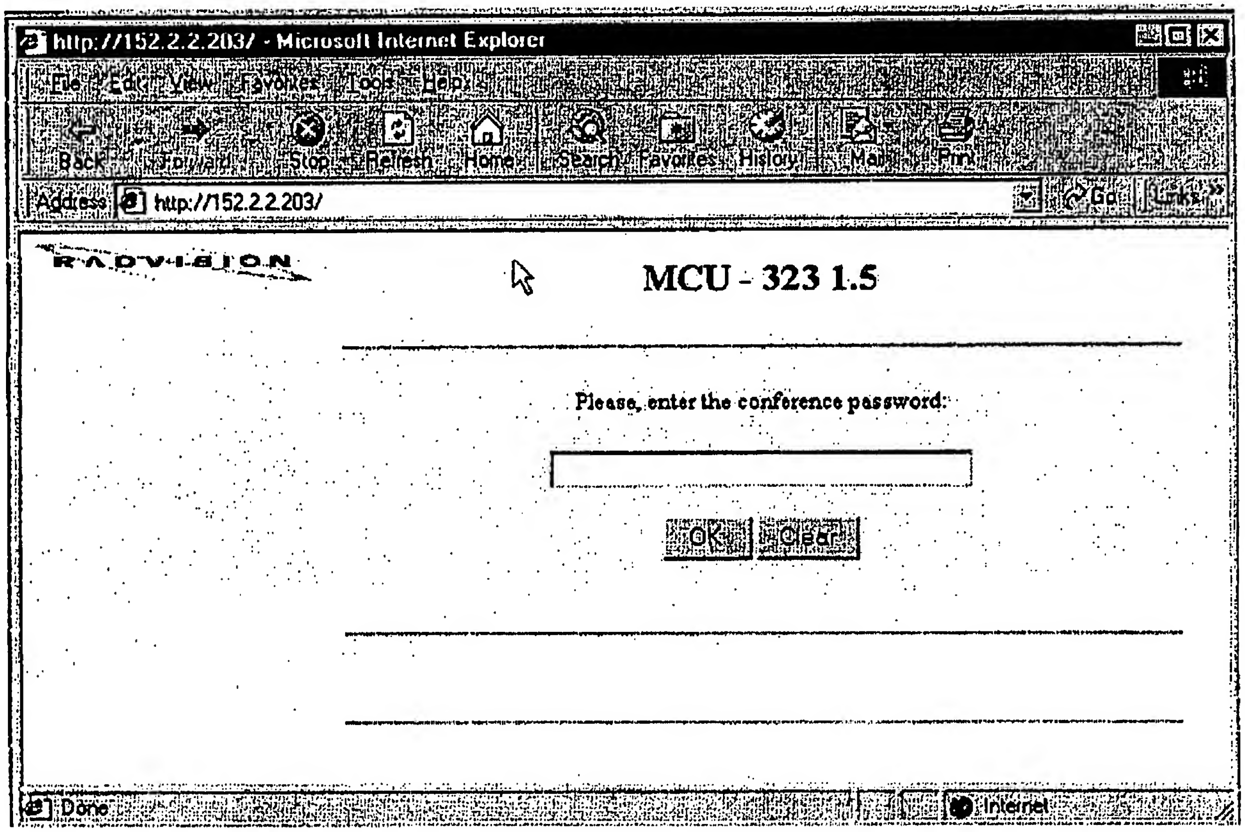
General application sharing and data collaboration instructions can be found in Instructions on Application Sharing and Data Collaboration. This material includes some additional information on what is required to start application sharing and data collaboration when in a multi-point call under a RadVision MCU and Gatekeeper.

Establishing the Data Share Group

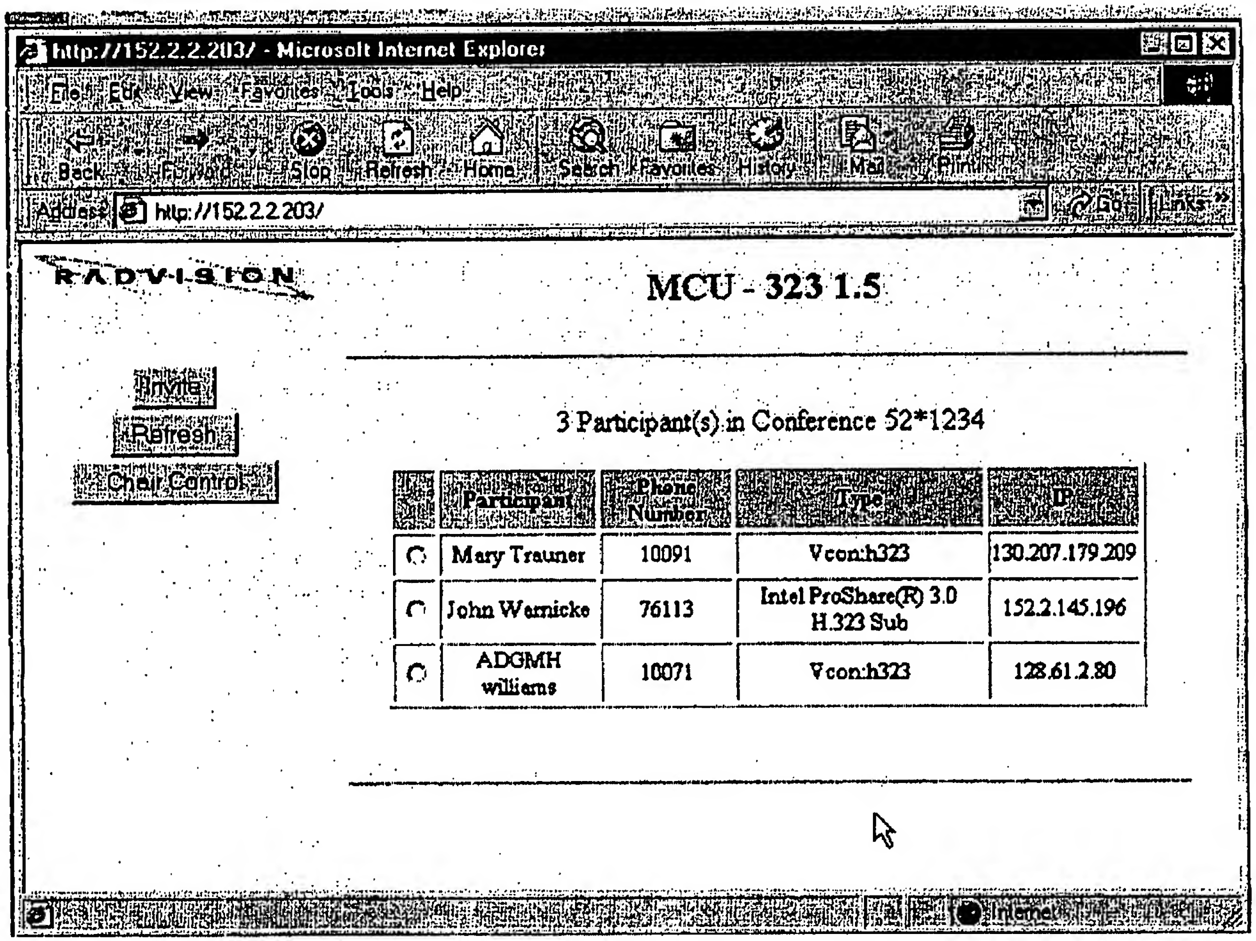
Since there will be three or more people in a multi-point conference, one person needs to bring all others into the MCU "Data Share" mode. (We'll call this person the share-lead.) To do this, the share-lead should start the Internet Explorer browser. (The interface does not work properly with Netscape; this *restriction* is being reported to RadVision.) The share-lead should then link to their MCU via its ip number. For this example

http://152.2.2.203

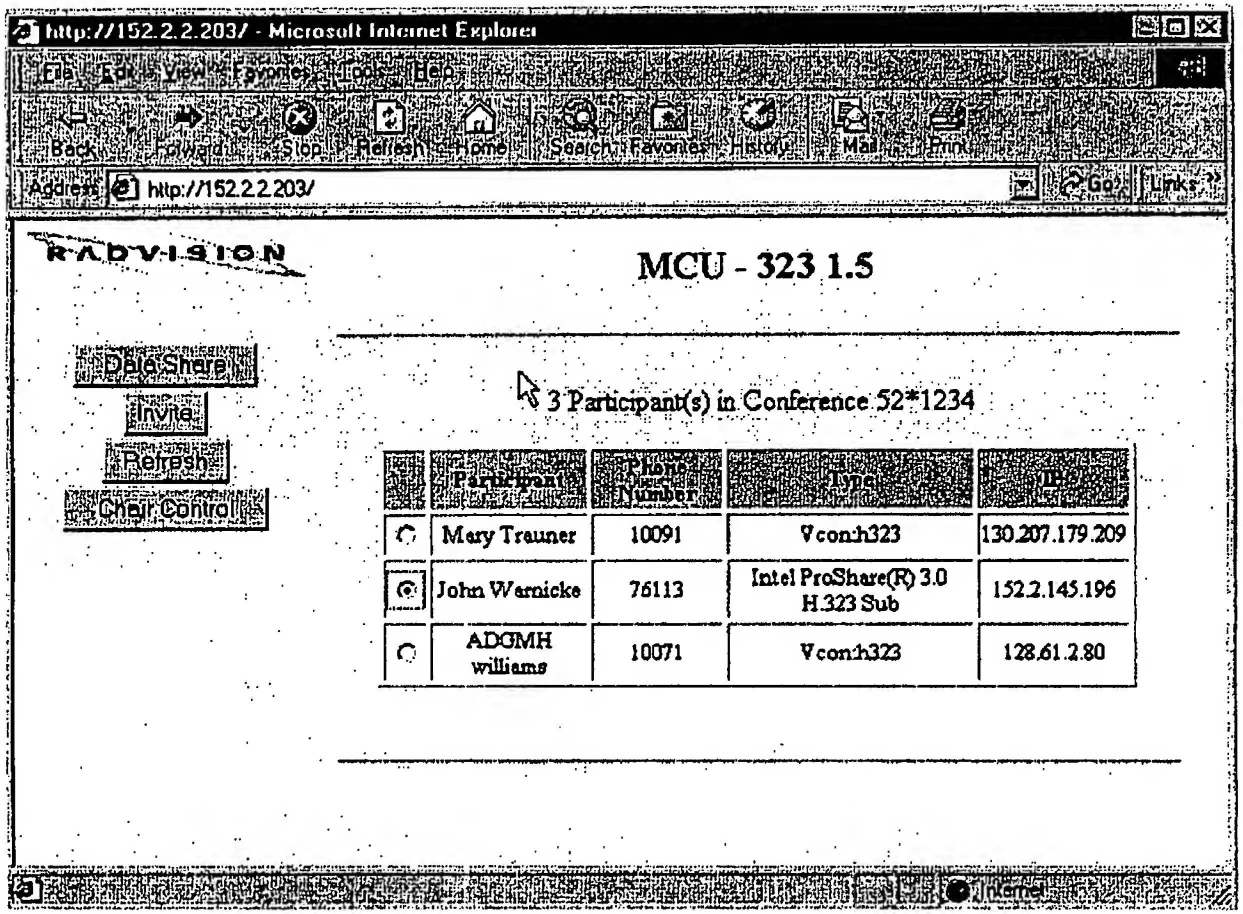
The MCU window will come up asking for a conference password.



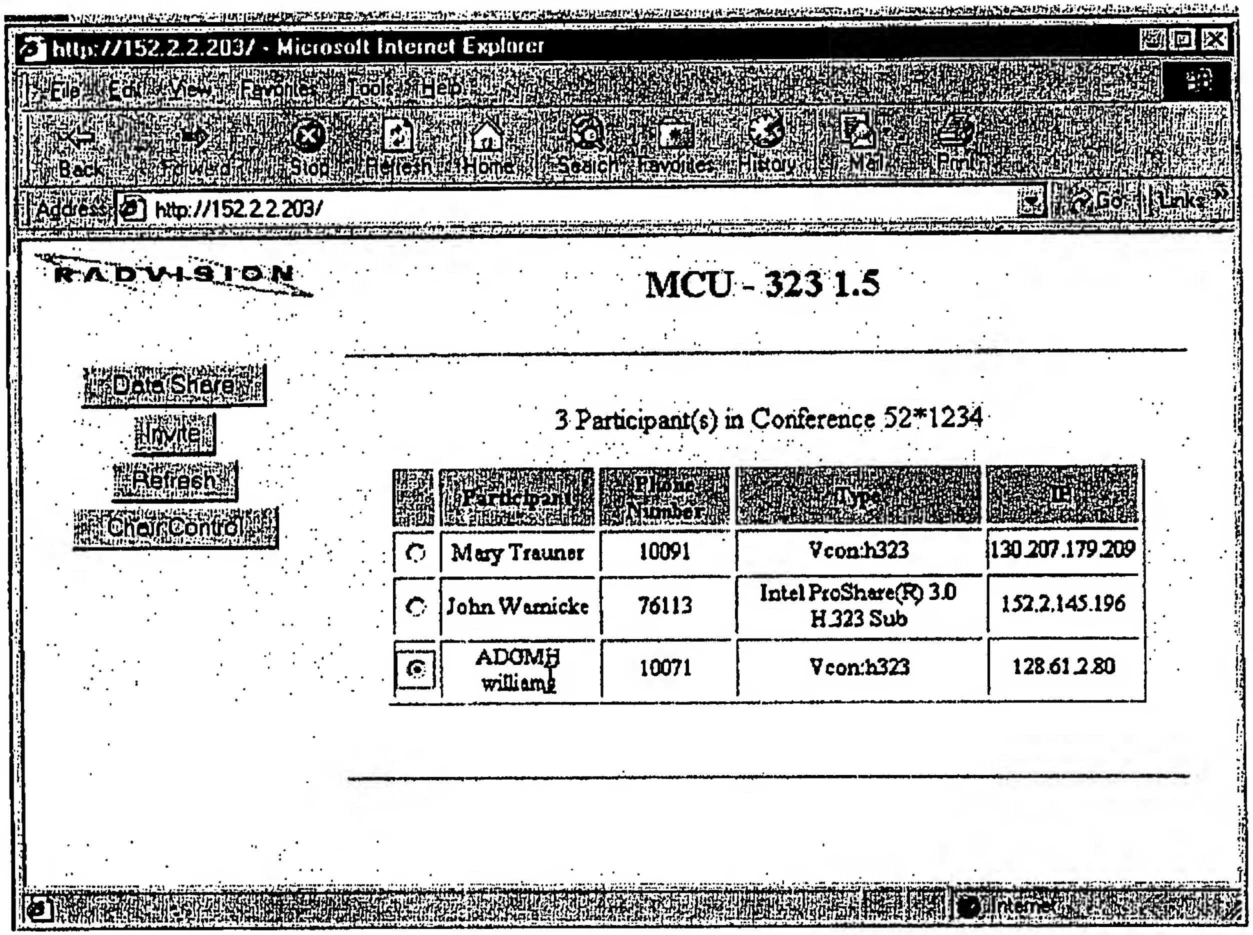
Enter that password (typically this is the same number that you dialed to reach the MCU) and click "OK". The window will show who is currently in the multipoint conference. (Note: This is not dynamic, therefore "Refresh" should be clicked every so often to see if anyone else has joined in or left.)



Each person currently in the conference is listed; a radio box appears to the left of each name. Let's say that Mary is the share-lead in this example. For each person with whom she wants to application share or data collaborate, she will click the radio box and then click "Data Share". First she will include John.



Then she will add in Williams.



If they are on VCON clients using the Standard Data Sharing, the VCON "Share" button scenario will be used. If NetMeeting is their application sharing choice, a NetMeeting window will appear on each screen as they are added to the Data Share. See Instructions on Application Sharing and Data Collaboration for further details on choosing applications and enabling sharing and/or collaboration under either of these options.

"File Transfer," Microsoft Windows Technologies Windows NetMeeting, last updated June 4, 1999,http://www.microsoft.com/windows/netmeeting/features/files/default.asp

Enter a search phrase:

Windows XP
Windows 2000 Home
Windows 2…
Windows 2000 Server
Windows 2000 Advanced Server
Windows 2000 Datacenter Server
Windows NT …
Windows NT Server 4.0
Windows Me
Windows 98
Windows 95
Embedded …
Windows CE .NET
Wi…
Windows Technologies
Internet Explorer

NetMeeting Home Page
Features
System Requirements
Reviews
Business Users
Home Users
Authors and Developers
Companion Products & Services

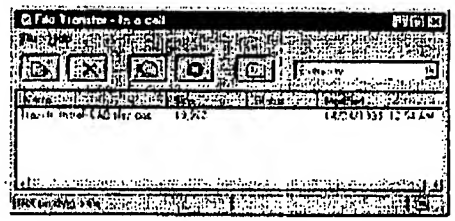
File Transfer

File transfer lets you send files during a NetMeeting conference.

With file transfer, you can:

- Send a file in the background to conference participants.
- Send the file to everyone in the conference, or to one or more selected participants.
- Accept or reject transferred files.

Learn more.



Last updated: Friday, June 04, 1999

Features Contents
Features Home
Video and Audio Conferencing
Whiteboard
Chat
Internet Directory
File Transfer
Program Sharing
Remote Desktop Sharing
Security
Advanced Calling

"From Dial Tone to Media Tone," Analyst: R. Mahowald, IDC, June 2002

5 Speen Street • Framingham, MA 01701 USA • Phone 508.872.8200 • Fax 508.935.4015 www.idc.com

IDC
Analyze the Future

From Dial Tone to MediaTone

How the WebEx Interactive Network Powers Business Communications to New Heights

Analyst: Robert Mahowald

OVERVIEW

While audio conferencing and static communications (e.g., email and telephone) rivaled face-to-face meetings as the most important forums for business meetings in the 1990s, Web conferencing — with its real-time multimedia communications, data sharing, and computer-telephony integration (CTI) — is poised to drive business communications in the new millennium. The dramatic uptake in demand means new opportunities for vendors of Web conferencing products.

IDC research points to the rapid adoption of Web conferencing in areas as disparate as sales, marketing, training, support, engineering, channel management, and internal employee communications. Findings from IDC's *2001 Conferencing Survey* show that current and planned buying is strong: An average of 43.6% of respondents reported they plan to increase their conferencing usage by 100% or more in the next six months, whereas only 1.5% plan to do less conferencing in the next six months.

But what is pushing the user numbers ever higher is the fact that Web conferencing is fast becoming a general-purpose communications service. Business users are increasingly looking at online conferencing to more effectively communicate with customers, prospects, suppliers, and partners. They are also using the technology in a way they had formerly reserved for the office water cooler — as a proxy for a gathering "place," a notional room for spontaneous conversation, discussion, and planning. People who entered the workplace during the 90s are as used to the PC interface as they are familiar with the telephone, and they display much the same comfort and facility with conducting a visual conversation using a computer as they do a voice conversation with a telephone handset.

While current use of Web conferencing is robust, IDC forecasts an even stronger future for this market. This growth prediction is based in part on the assumption that applications and services will be deployed on networks that are increasingly reliable, scalable,

Sponsored by WebEx

extensible, global, and cost efficient. As Web conferencing enters prime time in the enterprise, and vendors seek to differentiate themselves with new features, customers will not overlook the importance of the CTI networks that provide the open systems interconnect (OSI) layers critical to highly available, rock-solid conferencing systems.

IDC believes that MediaTone — and the WebEx Interactive Network it powers — is an example of the kind of "guarantee" that conferencing vendors and service providers need to make to customers.

WebEx's new multimedia switching platform is driven by the company's MediaTone communication signaling technology for sharing multimedia information and datastreams. IDC believes that MediaTone — and the WebEx Interactive Network (WIN) it powers — is an example of the kind of "guarantee" that conferencing vendors and service providers need to make to customers. Among all the other differentiators, the ability to provide "dial tone"-like quality of service assurances is part of what will take Web conferencing to new heights.

METHODOLOGY

This white paper highlights the opportunities for vendors of conferencing and related collaborative multimedia services. Further, this paper presents one vendor, WebEx, and its deployment platform, WebEx Interactive Network, as an example of a solution that addresses this opportunity.

This paper's focus is qualitative rather than quantitative; that is, we do not attempt to quantify the size of this market opportunity. Instead, we discuss the tremendous opportunity for vendors in this market segment and how clients can best leverage this opportunity.

INTRODUCTION

How are businesses meeting, communicating, and sharing information? The answer is complex. The kinds of meetings, the contexts, the participants, the information shared, and the results are evolving as technology races to develop ways for visual collaboration to rival — and sometimes be more efficient than — face-to-face meetings.

If we think about how verbal vocabulary has evolved to meet the changing needs and mores of its users, it is clear that it could only do so because it had a flexible but unchanging semantic structure — subjects, verbs, sentences, clauses — on which to hang the words.

If we think about how verbal vocabulary has evolved to meet the changing needs and mores of its users, it is clear that it could only do so because it had a flexible but unchanging semantic structure — subjects, verbs, sentences, clauses — on which to hang the words. As the lives of early humans grew more complex, more words were added to the language to accommodate the dynamism of the communication. This growth has progressed to the present day, and we now have more words than we can ever use to describe a myriad of complex situations, events, and concepts.

Communications technology has evolved along the same lines. The telephone, for example, has a basic structure. Our plain old telephone system (POTS) — physical cables, network switching centers, and

end-point devices in homes and offices — has provided a basic structure on which to build not only simple telephony features such as the ability to call any number in the world but also complex management features such as call waiting, voicemail, unified messaging, and conference calls. Like language with its structure, shared understanding of words, and ubiquity, the POTS had to be utterly reliable, simple to use, global in reach, and in almost every home and office.

It is important to understand the real vision of the builders of the original POTS voice network. They realized that they needed to build something tremendously flexible, extensible, and standards-based to accommodate any kind of innovation in the years to come.

It is important to understand the real vision of the builders of the original POTS voice network: Even though these early engineers had no idea what kind of voice services would be introduced in later years, they realized that they needed to build something tremendously flexible, extensible, and standards based to accommodate any kind of innovation in the years to come.

Although in 1880 there may have been some doubt as to whether Marconi's telegraph or Bell's telephone would win the right to play a seminal role in the lives of nearly every human being, the network built around the telephone, and the network effect to produce millions of network nodes (i.e., phones), brings us to where we are today.

We live in the age of the Internet. Corporate workers have become used to interacting with their PCs almost as they would with a colleague; much as the telephone handset became a physical proxy for the person on the other end of the line, PCs are an embodiment of how we in business communicate today, with email, instant messaging, calendaring and scheduling, and team collaborative applications. Browsers are increasingly our information communication devices, more than the telephone.

When CTI became possible in the early 1990s, technologists looked for ways to make a tighter link between data and voice and to build CTI products as reliable, useful, and ubiquitous as the telephone network. To date, CTI has brought us the uniting of voice, fax, and email messages in a common object store (unified messaging); interactive voice response (IVR); and numerous other linkages between the PC and the telephone.

But these are largely one-way products. They rely on the PC as a viewing device, or as a window into a network object store, and little more. Email is store-and-forward technology, unified messaging is "push" technology, and even instant messaging, with all its connotation of speed, cannot match the free-flowing spontaneity of a lively conversation.

MORE THAN MEETINGS

Both the profile of the typical Web conferencing user and the business areas in which Web conferencing is being used have evolved dramatically in the past few years. As conferencing services vendors deploy more specialized, high-touch features to address more meeting types, their use as substitutes for existing types of online communications has grown. Just three years ago, most conferences were audio only, and data sharing was a one-to-many activity, with limited user controls and no flexibility.

Today, the average user is not an "IT type." Users of most Web conferencing products don't have to go to special conference rooms or schedule time on the system with a gatekeeper in their company's telephony department.

Today, the average user is not an "IT type." Users of most Web conferencing products don't have to go to special conference rooms or schedule time on the system with a gatekeeper in their company's telephony department. As the technology has grown more linked to the desktop PC, control over meetings has been decentralized. Scheduling, attendance, richness of the information shared, and other issues are decided largely by the meeting's host, and users don't need to schedule a meeting so much as click a button to launch an ad hoc session.

How have meetings changed? Only a few years ago, many meetings were audio-only conference calls, handled by incumbent local exchange carriers (ILECs), and they were scheduled using a flood of telephone calls. When users needed to see something, they had to congregate in a single physical location. There was a place to go to for meeting and another place to go to for working. Users did their thinking offline, asynchronously, then arranged a call to convey decisions already made and strategy already formed.

Today, electronic meetings are about collaborating, sharing, and teaching. They are part of the process, not the end of the process.

Today, electronic meetings are about communicating, sharing, and teaching. They are part of the process, not the end of the process. Think of the new uses for conferencing today: salespeople conducting meetings with prospects and existing customers, customers and employees receiving training anywhere in the world, and experts providing live hands-on support to remote customers. While the first phase of business communications was face to face, the advent of the telephone enabled most communications to be remote, with fewer face-to-face meetings. This change dramatically increased business opportunities. Now, with the ubiquity of multimedia-based Web communications, users can rely on both telephone and visual capabilities to dramatically enhance the effectiveness of remote communications. This has the effect of further reducing the cost of doing business and more significantly increasing business opportunities, just as the telephone did over the last century.

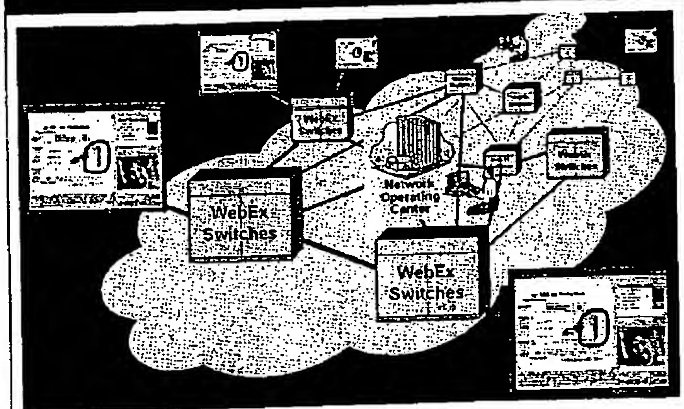
Salespeople use Web conferencing to present and deliver online demonstrations to customer prospects across the country. Instructors can reach students anywhere there is a Internet connection, with guided learning, feedback, and performance assessment — just like in the classroom. Engineers can share ideas with 3D computer-aided design (CAD) objects and get quick feedback. At one end, marketing can present new products to thousands of prospects, and at the other end, two colleagues can share the beginnings of a great new idea born from digital scribbles on a white board. Welcome to the wonderful world of Web conferencing.

WHERE NETWORK ARCHITECTURE FITS IN

Architecturally, conferencing links voice and data by providing a switching network that unites the public switched telephone network (PSTN) and the public Internet. The standard OSI model describes the seven layers on which communications data must be addressed for it to be successfully transported — from the miles of cables buried under highways and skyscrapers, through data and network synchro-

nization, session initiation, presentation (encryption and conversion), and, finally, up to the application layer, the user interface, and the PC (see Figure 1). It is a complex model, and while it is possible to combine certain layers, a weak link, or skipped layer, could mean a dropped call, a misrouted data file — in short, failed communication.

Figure 1: Network Architecture



Source: WebEx, 2002

One can imagine the machinations that must go on behind the scenes to produce a successful online meeting: As the audio portion moves along the PSTN, it passes several possible points of failure. Instructions from the user interface need to be transmitted via the packet-switching OSI layers — application, presentation, and session — where audio encounters Secure Sockets Layer (SSL) data encryption, decryption, and data conversion. Then, these two streams — audio and visual — have to meet seamlessly via a PSTN bridge and be transmitted to many users — all in real time.

When the telephone first emerged, Bell Systems dealt with this complexity by focusing on the redundancy and failover capacity of its network. The result is that the dial tone has become the sonic metaphor for global reach, utter reliability, high quality, and security. The network for Web conferencing has the same business requirements and attributes as the telephone system: Users want to be able to plug in a PC or mobile device and go, with the assurance that they will have dial-tone reliability no matter where on the Web their meeting takes them.

An added point of complexity comes from the fact that while the PC industry is relatively nascent, true CTI is even more new. Even top technologists don't know the bounds of the Internet, and the borders between data and voice are made ever fuzzier as voice moves to the Internet with voice over IP (VoIP). Because the horizon is always shifting, the network on which communications services are built needs to be immensely extensible — blind to the vagaries of different operating systems, platforms, devices, user types, and so on. It needs to be generic enough to not get in the way of the changing

uses, mobile platforms, and shifts in technology that are sure to come about in the next 25 years.

WEBEX OVERVIEW

WebEx (NASDAQ: WEBX), based in San Jose, California, provides a communications infrastructure for real-time business meetings on the Web. WebEx's products are carrier-class communications services that integrate voice, video, and data to enable collaboration, information and process sharing, and training. These services are based on WebEx's multimedia switching platform. WebEx services enable end users to share presentations, documents, applications, voice, and video on Windows, Macintosh, or Solaris systems, and they can be accessed via a Web browser. These services are used across the enterprise in such functions as sales, support, training, marketing, and engineering.

WebEx is now delivering these services to more than 6,100 corporate accounts through 200 different distribution channels.

NETWORK TOPOLOGY AND THE WEBEX INTERACTIVE NETWORK

When you understand how visual meetings, conferences, and etraining sessions are delivered, the dial-tone analogy really begins to ring true. Web meetings are a Web-based extension of audio communications, and in almost all cases, audio accompanies the visual portion of the session. Audio can be delivered via the network of a local telephone service provider or a larger carrier such as AT&T, France Telecom, or WorldCom. In many cases, voice services are delivered by the provider of the visual conferencing, or they can be offered using Internet protocols (IP), so that the POTS is bypassed entirely. Many current Web conferencing industry leaders allow for a variety of options, and participants on a call may use a combination of POTS and IP voice to synch up with the visual portion of the meeting.

The key point is that providers are gradually moving more of the controls for these services to the Web interface. Scheduling is increasingly accomplished via a browser-based interface. Dual-tone multifrequency (DTMF) controls within the Web interface let users manage and manipulate the audio part of the call using Web consoles. Because Web conferencing began as a marriage of new companies offering Web-based software products and services and existing vendors selling telephony services, it is tempting to think of Web conferencing as strictly a software business, with the telephony integration an afterthought.

Just as the original POTS architects needed to build a foundation for any future innovations in voice services, engineers building today's data networks find themselves faced with complex choices about building a network to deliver combined voice and visual services.

But telephony integration is perhaps the most intricate piece in the whole conferencing puzzle. Just as the original POTS architects needed to build a foundation for any future innovations in voice services, engineers building today's data networks find themselves faced with complex choices about building a network to deliver combined voice and visual services.

To deliver these communications services reliably and with predictable global performance, WebEx has deployed its own global network: the WebEx Interactive Network (WIN). WIN is composed of the application, presentation, and session functions (OSI Layers 5–7), with high-speed connections to the Internet on one end and voice bridges to the PSTN on the other end.

WIN is a network of WebEx multimedia communication switches that are architecturally distributed and highly scalable. The WebEx switches have substantial innovations that are rooted in WebEx's philosophy that conferencing is essentially a communications service, not a software application, and therefore has the same requisite business requirements and quality of service demands as the telephone network.

By leasing IP lines worldwide, WebEx has created a fully meshed network to ensure fault tolerance and rerouting in times of high use. The company has leased lines connecting communication hubs at colocation facilities that are distributed across the United States, Europe, and Asia/Pacific and has been expanding its global reach. Configured as a distributed network similar to phone networks, each hub is architected to be scalable and extensible. Each communication hub contains clusters of switches, ensuring high levels of reliability, redundancy, and scalability. As hubs are added,the regional hubs will act as contingency sites for each other, delivering what WebEx terms global "rings of service." WebEx's network will provide continuous reliability benefits because each additional node provides additional capacity, added paths for reliability, and reduced reliance on public networks.

Through WIN and the WebEx switching platform, information can be shared globally in an instant.

Through WIN and the WebEx switching platform, information can be shared globally in an instant. This guarantees reliability by controlling the network and by automatically routing and rerouting information based on network performance. Participants connecting with WebEx are automatically connected through the nearest WIN communications node, eliminating numerous network Internet service provider hops that are typically required. Should performance through a particular communications hub begin to degrade, alternate regional servers will be automatically pinged, and the next request will be routed through the nearest alternate server with the best performance level. These routing and rerouting capabilities ensure high levels of service for WebEx customers. These measures allow WebEx to guarantee fast and accurate delivery of information, strengthening the company's ability to alter current business methods.

Although WIN has been continually optimized and upgraded since its introduction two years ago, WebEx is moving toward even greater guarantees of reliability and scalability with the announcement of its major communications services infrastructure upgrade, MediaTone.

MediaTone

The Internet is increasingly crowded and unreliable. Packets of data and voice information may leave a gateway with great speed and determination, only to be blocked by least-common routing and Internet traffic. Packets may arrive at their destinations scrambled, late, or not at all, and because of the added complexity of bridging voice from a separate (PSTN) system onto Internet data, the points of possible failure become almost infinite.

Building on its existing support of a rich set of data, video, and audio capabilities, MediaTone has enabled WebEx to provide new capabilities that only a switched based network infrastructure can deliver.

WebEx's new MediaTone switching technology allows the WebEx switching platform to share complex media types, deliver advanced communications functionality, and support a range of new devices and platforms. The MediaTone signaling technology is part of Layer 6 (presentation layer) of the IP-based communications network layers and specifically provides the capability for real-time delivery and synchronization of multimedia content. Building on its existing support of a rich set of data, video, and audio capabilities, MediaTone has enabled WebEx to provide new capabilities that only a switched based network infrastructure can deliver, including:

- Support for Universal Communications Format (UCF) (UCF is WebEx's protocol for sharing rich media content within PowerPoint presentations in a way that lets users completely control the delivery. Full animation support is provided.)
- Sharing of embedded Flash files, with the ability to control start, stop, and pause files
- Sharing of Windows Media Player/RealPlayer content, with the ability to start, stop, and pause delivery to all participants
- Sharing of CAD and other 3D objects, with full manipulation
- Sharing of previously recorded WebEx meetings
- Secure access to or sharing of information in a meeting, whether the content is local or remote
- Multipoint videoconferencing, from either a browser or in support of Polycom cameras and standard video camcorders
- Access to presentations using handheld and wireless devices, with the ability to participate in meetings
- Simultaneous sharing of multiple documents or presentations; viewing of multiple documents at the same time, with the ability to flip back and forth between them

But is all of this really important if, as we said earlier, the average user is not an IT type? Web conferencing technology has trickled down from IT to desktop users, and it is now a part of the lives of most knowledge workers. Users see a user interface, and they have user-operated controls. Why is the network important to them?

All the bits and pieces assembled to link the PSTN and the Internet and to deliver voice, video, and data reliably, globally, and flexibly are important because if a system is down just once, drops calls, or doesn't accommodate specific situations and needs, then it is dead in the water. Disenchanted customers are like flowing water: They will find another path to their goal should one way be blocked.

WEBEX COMMUNICATIONS SERVICES

WebEx offers multiple communications services to fulfill diverse user needs within enterprises. Services include:

- **Meeting Center** provides rich interactive meeting environment.
- **Event Center** (formerly OnStage) enables delivery of multimedia Web seminars.
- **Support Center** (formerly OnCall) enables delivery of remote, hands-on technical support.
- **Training Center**, which is WebEx's newest service and the first to be based on MediaTone, enables remote delivery of live training to customers and employees.

CHALLENGES

A key challenge to overall adoption of Web conferencing is that several related applications and services deliver parts of the promise of real-time conferencing without all the pieces. For example, for most knowledge workers, the inbox paradigm is very strong. For small businesses, or firms with employees, partners, and customers relatively proximate, email, telephone, and other means of communication may continue to suffice. For larger businesses, where customers, prospects, partners, and employees are more geographically dispersed, however, communications beyond the telephone are essential.

The true barriers to entry in the market are far higher for vendors seeking to serve the marketplace as global communications service providers.

At first glance, the cost of developing Web conferencing products seems low. A few employees writing code can write a Web application server to store and share limited forms of information. The true barriers to entry in the market are indeed far higher — especially for vendors seeking to serve the marketplace as global communications service providers. Worldwide reach and reliability require a global network with peering agreements, impeccable code, built-in security, high scalability, rich functionality, and an army of client service representatives to meet the standard for 24 x 7 service that is increasingly expected of conferencing service providers. WebEx has had to invest substantially in its switching platform, WIN, and MediaTone signaling technology in the past few years, and the cost of acquiring new customers remains high.

Vendors such as WebEx face competition from a growing pool of Web conferencing product and services suppliers.

WebEx's continued demonstration of dial-tone reliability is important if it is to convince new customers that it can deliver the kind of Web conferencing capability and uptime they require.

CONCLUSION

The promise of dynamic, cost-effective, real-time, and productive Web-based communications is real. IDC's *2001 Conferencing Survey* revealed that 82% of businesses with more than 500 employees use some type of conferencing application. Buyers will continue to be drawn by the tremendous potential return on investment that they can realize through savings on equipment, bandwidth, personnel, and applications licenses, as well as sharply reduced travel costs.

But the real promise of Web conferencing is that it takes the dream of the telephone and extends it far beyond voice. Customers expect rapid responses. Competition pushes businesses to plan, design, implement, and support products on a 24 x 7 basis. Therefore, talk is not enough. To lead, businesses need to show, link, exchange, demonstrate, teach, relate, and collaborate. As business cruises along at Internet speed, users will increasingly need to share rich digital files, demonstrate products, confer with colleagues, and teach customers in real time. And they will need to perform such tasks from multiple types of emerging portable IP devices.

WebEx provides a comprehensive solution based on its communications services, infrastructure, and worldwide network. Demand for these services will continue, and reliable, scalable, extensible, and ubiquitous services such as WebEx's will be among the winners at the forefront of this shift as adoption of real-time multimedia communications continues to grow.

The compelling nature of what WebEx has accomplished is reflected in its having earned 5,000 corporate customers and more than doubled revenue in each of the past two years.

The compelling nature of what WebEx has accomplished is reflected in its having earned 5,000 corporate customers and more than doubled revenue in each of the past two years. WebEx's reseller relationships with a number of key telecommunications vendors (including AT&T, MCI WorldCom, NTT, France Telecom, and Telia) highlight the reputation WebEx commands. WebEx's approach — looking at Web-based, real-time, interactive Web services as a communication technology and infrastructure issue rather than a software tool or application — will enable both the company and its MediaTone technology to power business communications to new heights.

IDC Worldwide Offices

CORPORATE HEADQUARTERS

IDC
5 Speen Street
Framingham, MA 01701
United States
508.872.8200

NORTH AMERICA

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario M5C 2C5 Canada
416.369.0033

IDC California (Irvine)
18831 Von Karmen Avenue
Suite 200
Irvine, CA 92612
949.250.1960

IDC California (Mountain View)
2131 Landings Drive
Mountain View, CA 94043
650.691.0500

IDC New Jersey
75 Broad Street, 2nd Floor
Red Bank, NJ 07701
732.842.0791

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212.726.0900

IDC Texas
100 Congress Avenue
Suite 2000
Austin, TX 78701
512.469.6333

IDC Virginia
8304 Professional Hill Drive
Fairfax, VA 22031
703.280.5161

EUROPE

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
Vienna A-1040, Austria
43.1.50.50.900

IDC Benelux (Belgium)
Boulevard Saint Michel 47
1040 Brussels, Belgium
32.2.737.76.02

IDC Denmark
Omagade 8
Postbox 2609
2100 Copenhagen, Denmark
45.39.16.2222

IDC Finland
Jarrumiehenkatu2
FIN- 00520 Helsinki
Finland
358.9.8770.466

IDC France
Immeuble La Fayette 2
Place des Vosges Cedex 65
92051 Paris la Defense 5, France
33.1.49.04.8000

IDC Germany
Nibelungenplatz 3, 11th Floor
60318 Frankfurt, Germany
49.69.90.50.20

IDC Italy
Viale Monza, 14
20127 Milan, Italy
39.02.28457.1

IDC Netherlands
A. Fokkerweg 1
Amsterdam1059 CM, Netherlands
31.20.6692.721

IDC Portugal
c/o Ponto de Convergancia SA
Av. Antonio Serpa 36 - 9th Floor
1050-027 Lisbon, Portugal
351.21.796.5487

IDC Spain
Fortuny 18, Planta 5
28010 — Madrid
Spain
34.91.787.2150

IDC Sweden
Box 1096
Kistagangen 21
S-164 25 Kista, Sweden
46.8.751.0415

IDC U.K.
British Standards House
389 Chiswick High Road
London W4 4AE United Kingdom
44.208.987.7100

LATIN AMERICA

IDC Latin America
Regional Headquarters
8200 NW 41 Street, Suite 300
Miami, FL 33166
305.267.2616

IDC Argentina
Trends Consulting
Rivadavia 413, Piso 4, Oficina 6
C1002AAC, Buenos Aires, Argentina
54.11.4343.8899

IDC Brazil
Alameda Ribeirao Preto, 130
Conjunto 41
Sao Paulo, SP CEP: 01331-000 Brazil
55.11. 3371.0000

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 13
Providencia
Santiago, 9, Chile
56.2.334.1826

IDC Colombia
Carerra 40 105A-12
Bogota, Colombia
571.533.2326

IDC Mexico
Select-IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo Condesa
C.P. 06100, Mexico
525.256.1426

IDC Venezuela
Calle Guaicaipuro
Torre Alianza, 6 Piso, 6D
El Rosal
Caracas, Venezuela
58.2.951.1109

CENTRAL AND EASTERN EUROPE

IDC CEMA
Central and Eastern
European Headquarters
Male Namesti 13
110 00 Praha 1
Czech Republic
420.2.2142.3140

IDC Croatia
Srednjaci 8
1000 Zagreb
Croatia
385.1.3040050

IDC Hungary
Nador utca 23
5th Floor
H-1051 Budapest Hungary
36.1.473.2370

IDC Poland
Czapli 31A
02-781 Warszawa, Poland
48.22.7540518

IDC Russia
Suites 341-342
Orlikov Pereulok 5
Moscow, Russia 107996
7.095.975.0042

MIDDLE EAST AND AFRICA

IDC Middle East
1001 Al Etihad Building
Port Saeed
P.O. Box 41856
Dubai, United Arab Emirates
971.4.295.2668

IDC Israel
4 Gershon Street
Tel Aviv 67017, Israel
972.3.561.1660

IDC South Africa
Building 9, Pebble Beach
Fourways Golf Park
Roos Street
Fourways, Gauteng
South Africa
27.11.540.8000

IDC Turkey
Tevfik Erdonmez Sok. 2/1 Gul
Apt. Kat 9D
46 Esentepe 80280
Istanbul, Turkey
90.212.275.0995

ASIA/PACIFIC

IDC Singapore
Asia/Pacific Headquarters
80 Anson Road
#38-00 IBM Towers
Singapore 079907
65.6226.0330

IDC Australia
Level 3, 157 Walker Street
North Sydney, NSW 2060
Australia
61.2.9922.5300

IDC China
Room 611, Beijing Times Square
88 West Chang'an Avenue
Beijing 100031
People's Republic of China
86.10.8391.3610

IDC Hong Kong
12/F, St. John's Building
33 Garden Road
Central, Hong Kong
852.2530.3831

IDC India Limited
Cyber House
B-35, Sector 32, Institutional
Gurgaon 122002
Haryana India
91.124.6381673

IDC Indonesia
Suite 40, 17th Floor
Jakarta Stock Exchange
Tower 2, Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
6.221.515.7676

IDC Market Research (M) Sdn Bhd
Jakarta Stock Exchange Tower II
17th Floor
Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
62.21.515.7676

IDC Japan
The Itoyama Tower 10F
3-7-18 Mita, Minato-ku
Tokyo 108-0073, Japan
81.3.5440.3400

IDC Korea Ltd.
Suite 704, Korea Trade Center
159-1, Samsung-Dong
Kangnam-Ku, Seoul, Korea, 135-729
822.551.4380

IDC Market Research (M) Sdn Bhd
Suite 13-03, Level 13
Menara HLA
3, Jalan Kia Peng
50450 Kuala Lumpur, Malaysia
60.3.2163.3715

IDC New Zealand
Level 7, 246 Queen Street
Auckland, New Zealand
64.9.309.8252

IDC Philippines
703-705 SEDCCO I Bldg.
120 Rada cor. Legaspi Streets
Legaspi Village, Makati City
Philippines 1200
632. 867.2288

IDC Taiwan Ltd.
10F, 31 Jen-Ai Road, Sec. 4
Taipei 106
Taiwan, R.O.C.
886.2.2731.7288

IDC Thailand
27 AR building
Soi Charoen Nakorn 14,
Charoen Nakorn Rd., Klongtonsai
Klongsan, Bangkok 10600
Thailand
66.02.439.4591.2

IDC Vietnam
Saigon Trade Centre
37 Ton Duc Thang Street
Unit 1606, District-1
Hochiminh City, Vietnam
84.8.910.1233; 5

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and ebusiness trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, ebusiness companies and the financial community. Additional information can be found at www.idc.com.

IDC is a division of IDG, the world's leading IT media, research and exposition company.

02-146SOFTWA3381
June 2002

IDC
Analyze the Future

www.idc.com

"MediaTone - The 'Dial Tone' for Web Communications Services,"
Webex, 2003

webex™

MEDIATONE™

The "Dial Tone" for
Web Communications Services

The "Dial Tone" for Web Communications Services

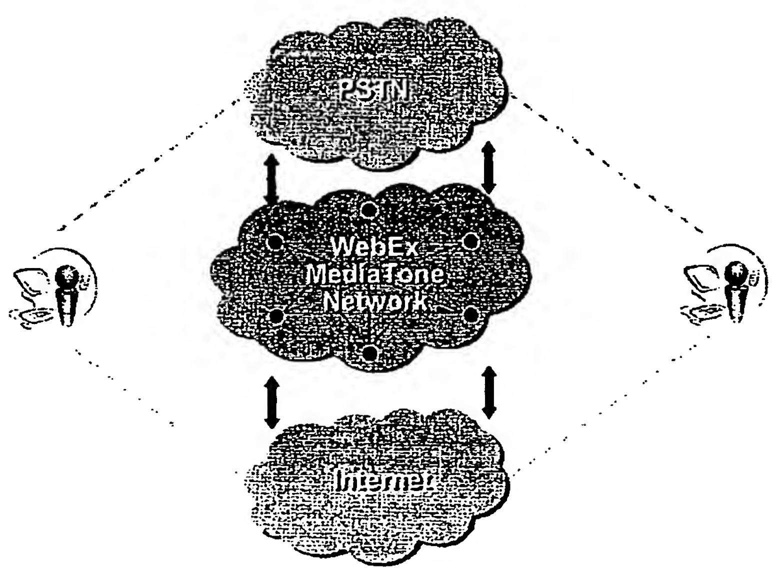
WebEx™ MediaTone™ technology enables WebEx meeting participants worldwide to enjoy the richest set of data, voice and video interactive services together with unparalleled network performance and reliability. The secure, highly scalable MediaTone Network can support millions of simultaneous calls, and as many as 5,000 individuals may attend one meeting.

The WebEx MediaTone Platform positions WebEx as the technological leader in Web communications services, providing OEM services to WebEx partners and industry-leading meeting services to nearly 7000 corporations. The MediaTone architecture provides ubiquitous access—regardless of location, hardware platform, operating system, browser, and wired or wireless status—enabling everyone to reap the benefits of online meetings.

MediaTone Technology

All WebEx services integrate the company's MediaTone technology. This proprietary technology enables true interactive communication sessions with levels of functionality, reliability, security and scalability impossible to achieve in a database-centric, store-and-retrieve architecture. With its modular framework and standards-based application programming interfaces (APIs), MediaTone is the "dial-tone" for Web communications.

The highly extensible WebEx architecture includes two components: the MediaTone Network and the MediaTone Platform.



We've got to start meeting like this.™

Customer Requirements

As they evaluate solutions that can deliver such benefits, customers factor in many technical and business requirements. These include the need for:

- A flexible, scalable, reliable Web services architecture with powerful and extensible capabilities.
- The ability to accommodate millions of people-minutes in online meetings.
- Reliable third-party service provision for integrated rich-media calls across enterprises.
- Integration with the customer's enterprise IT infrastructure and support for heterogeneous environments *(eg. Microsoft Exchange/Outlook and Domino/Notes integration, Instant Messaging, Portals).*
- Support for diverse online meeting scenarios (e.g., sales, marketing, training, support, project management, design reviews).
- Rapid deployment and ease of administration.
- Security that addresses authentication, encryption, auditing and tracking.
- Full support for ad-hoc and scheduled sessions.
- Integration with billing and reporting systems.
- Support for personalization.
- Seamless integration with voice systems such as audio conferencing bridges and Voice over IP (VoIP) solutions.
- Worldwide 24x7x365 support and native language support.

MediaTone Network

The MediaTone Network is a fully redundant, high-performance private global network specifically designed to deliver Web communications services. Created with a carrier-class information-switching architecture, the MediaTone Network delivers optimal performance by routing communications across several WebEx data centers. The result is a high-performance network that is unmatched for secure, reliable, fast, real-time Web communications. WebEx is the only company to develop and deploy a globally distributed information-switching network specifically designed for the delivery of interactive Web communications services.

With the WebEx MediaTone Network:

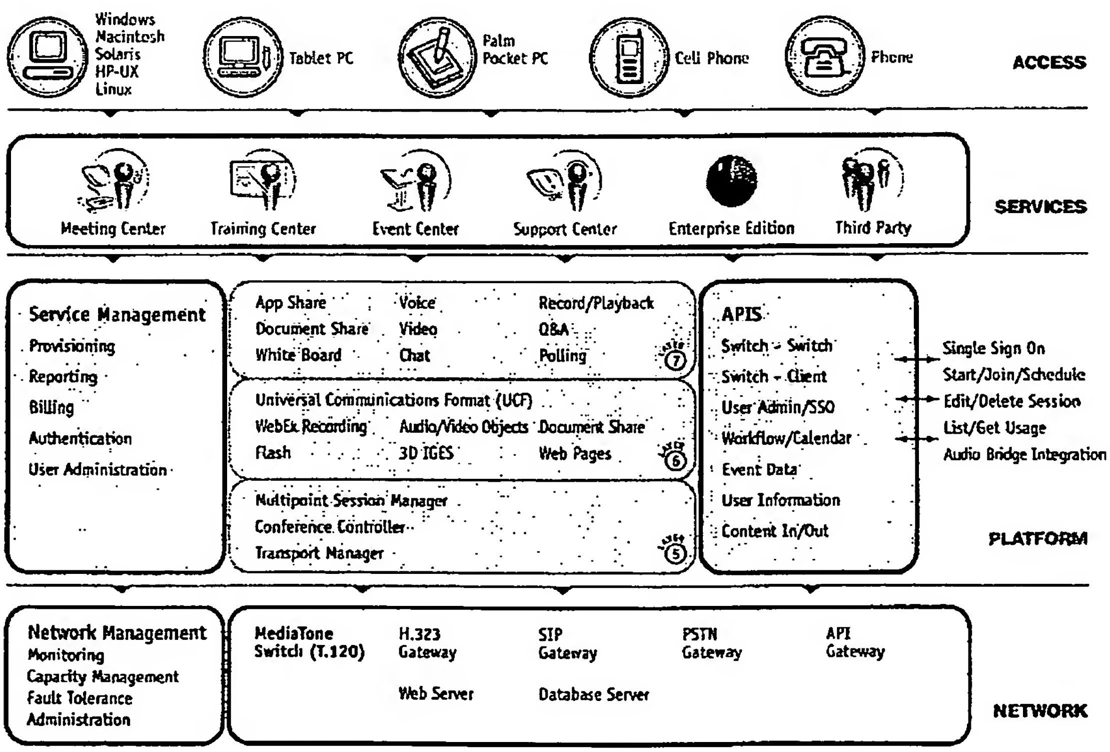
- Latency and interruptions in multi-point interactive meetings are eliminated, even when participants are located in different countries.
- Participants may use any telephone for the audio portion of their meeting.

MediaTone Platform

The MediaTone Platform, a distributed software architecture for Web-based communications services, is deployed over the MediaTone Network. The MediaTone Platform supports the full range of data, voice and video communications needed to provide a setting that simulates the full spontaneity and productivity of face-to-face meetings. With the MediaTone Platform, WebEx can rapidly develop new interactive Web communications services.

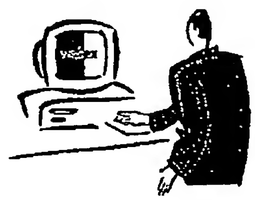
The MediaTone Platform Provides:

- Administrative capabilities, such as scheduling, provisioning and billing.
- Capabilities for session management, conference control and communications.
- Rich features, such as application sharing, video, white boarding and VoIP.



WebEx MediaTone Architecture

A More Robust T.120



The MediaTone Platform leverages the T.120 standard, which supports platform-independent, multi-point data communications. WebEx has built upon the T.120 standard, adapting it to a Web-native infrastructure and significantly enhancing the T.120 Presentation and Application Layers. WebEx also has extended the T.120 protocols for scalability, fault tolerance, security and manageability—while assuring PSTN integration. By basing the MediaTone Platform on an enhanced version of the T.120 standard and by creating a set of integration toolkits, WebEx has created a highly scalable and open information-switching network.

Originally developed by leading telecommunications providers to promote Integrated Services Digital Network (ISDN) service, T.120 is the first well-defined switched architecture for real-time data communications. The standard addresses multimedia-technology issues with attention to both voice and data requirements. The T.120 protocol, which focuses on Layers 5-7 of the OSI Model, addresses the following issues:

- Communications/transport interface (e.g., TCP/UDP).
- Multipoint session management and conference control.
- Application Layers standards.
- White boarding, application sharing and file transfer.

WebEx enhancements to the T.120 protocol suite include:

- Well-defined support for HTTP.
- Vector-based graphic format for sharing any document/format and session archiving.
- Format and protocol for sharing and synchronizing rich media.
- Federated Switched Network for global deployment and ubiquitous access.
- PSTN integration.
- A rich set of APIs and tools for integration with Web and desktop applications.
- Enhanced network scalability, reliability and manageability.
- Improved security.
- Business and operational tuning.

Service Management Layers

WebEx service management layers provide customers with an extensive array of features to maximize the use of WebEx services. WebEx service management capabilities include:

- Administration.
- Reporting and Monitoring.
- Fault/Recovery.
- Provisioning and Billing.
- Authentication.

The OSI Model

The OSI communications model defines how messages should be transmitted between any two points in a telecommunication network. The reference model defines seven layers of functions that take place at each end of a communication. Within the OSI Model:

- The ***Application Layer*** represents the level at which applications access network services, such as software for file transfers, database access and electronic mail.
- The ***Presentation Layer*** translates data from the Application Layer and manages security issues by providing services such as data encryption and compression.
- The ***Session Layer*** enables two applications on different computers to establish, use and end a session.
- The ***Transport Layer*** handles error recognition and recovery. It also repackages long messages, when necessary, and sends receipt acknowledgments.
- The ***Network Layer*** addresses messages and translates logical addresses and names into physical addresses. It also determines the routes and manages traffic problems.
- The ***Data Link Layer*** packages raw bits from the Physical Layer into frames— logical, structured packets for data.
- The ***Physical Layer*** transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium.

A Secure Network-Friendly Solution

WebEx patent pending technologies provide universal access to the MediaTone servers from the Internet. WebEx provides a secure location on the Internet where users can connect and collaborate at any time from any place without requiring modifications to their security infrastructure.

WebEx provides encryption of all session content with Secure Sockets Layer (SSL) technology to ensure the high level of security required for enterprise data communications. The T.120 based MediaTone architecture ensures that session contents are switched through the MediaTone Network and never stored in the WebEx infrastructure.

"WebEx Event Center and Meeting Center services enable VeriSign to present important new product information to our affiliates more effectively and efficiently. Our professional services group has increased productivity by providing quality support to our customers around the globe in far less time. WebEx provides the collaboration and presentation power required to fully support our outsourced service."

Stephen Fridakis, director of professional services, VeriSign

Additional Key Capabilities of the MediaTone Platform

WebEx Universal Communications Format (UCF)

- UCF is a part of the MediaTone technology developed by WebEx that makes interactive communication powerful and effective by delivering unprecedented levels of interactivity and support for advanced multimedia communications.
- UCF technology includes a portable document format for sharing and annotating on any document, and a protocol for sharing multimedia content.
- UCF enables the ability to:
  - Share PPT presentations with animations and transitions.
  - Spontaneously show rich media in WebEx meetings.
  - Easily create engaging, interactive presentations containing rich media.
  - Share Flash animation, video, audio, Web pages, and WebEx recordings in WebEx meetings with full control over delivery.

"With WebEx we're able to train hundreds of people at any given point in time. The employee never has to leave the branch. So the branch does not lose the productivity of the employee. And we wind up with a better-trained employee. We've estimated that this is saving us more than $4 million dollars per year."

Ron Schneider, First Vice President of training and performance development, Countrywide Wholesale Lending Division

WebEx Access Anywhere™

The WebEx Access Anywhere service enables any meeting participant to securely access or share information or applications that reside on an unattended remote computer. Mobile employees can access information on their office computers from a personal digital assistant (PDA) and share it in a WebEx meeting.

Video Conferencing

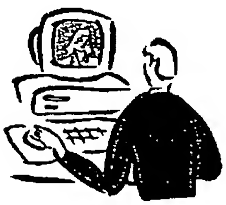
WebEx technology supports video conferencing with a browser and Webcams. WebEx also supports feeds from video technologies, including Polycom cameras and standard video camcorders. MediaTone also provides support for multi-point video conferencing.

The WebEx Solution

WebEx has developed a comprehensive set of Web communications services built on its patented MediaTone technology in order to meet the diverse requirements of its enterprise customers, enterprise portal providers, application developers and telecommunications providers. All WebEx services support highly interactive data, voice and video communications across multiple client platforms:

- Windows 95, 98, ME, NT, 2000 and XP, Tablet PC
- Macintosh OS 9 and OS X
- Solaris 7 and 8, HP-UX 11.3, Linux
- Palm OS, Pocket PC

Integrating WebEx Services with Enterprise Applications



Customers can integrate WebEx services with their enterprise applications by using the WebEx integration technologies. These include APIs and software development kits (SDKs) that support integration of real-time interactive capabilities with applications such as enterprise portals, project management services, content management solutions, and learning management systems using the popular Web programming languages HTML/XML. More than 350 companies and partners have integrated their applications with the MediaTone Platform.

The WebEx APIs, together with MediaTone's support for voice/data standards and protocols, provide many benefits for corporate customers and end users of WebEx services. Upon integrating their applications with WebEx services, corporations gain powerful Web collaboration capabilities that drive productivity and reduce travel costs. In addition, the ability to integrate WebEx services with corporate accounting, CRM, ERP, human resources and other key applications streamlines maintenance and upkeep. For end users, participating in WebEx online meetings is easy and efficient; single sign on integration eliminates the need for multiple passwords, and the user can easily move between applications or documents, as the meeting requires.

WebEx Integration Capabilities

The WebEx APIs and SDKs enable the following integration capabilities for enterprise customers and teleconferencing service providers:

To manage user data:

- Sign up new user
- Login/logout
- Activate/deactivate users
- Edit users

To manage meeting scheduling and registration:

- Start/schedule/host/join
- Edit/delete
- List/add/delete attendees
- Create/get registration form
- Register attendee

To manage and access the history of online sessions:

- List/get usage history
- List recorded access history

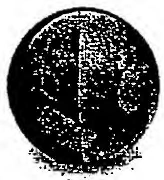
Protocol Support

MediaTone technology supports many multimedia protocols to fulfill its mission of delivering rich-media contents to the broadest possible selection of customer devices. Supported standards and protocols include:

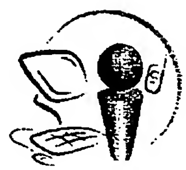
- H.323, the leading protocol for VoIP.
- Session Initiation Protocol (SIP), which is used for conferencing via IP phone or instant messenger (IM) device.
- Lightweight Directory Access Protocol (LDAP), a vendor-independent network directory protocol that provides directory-server integration for WebEx services.
- Extensible Markup Language (XML).
- SSL.
- Aviation Industry CBT Committee (AICC) protocol.
- SCORM.

In addition, WebEx supports the Universal Communication Format™ (UCF)—a revolutionary delivery format that enables high-speed sharing and delivery of rich content as part of a presentation. UCF enables users to share content within Microsoft™ PowerPoint™ presentations, with full control over the delivery. Users can share full PowerPoint animation and transitions, just as they would in an in-person meeting, and participants may start, stop or pause the streaming content whenever they desire.

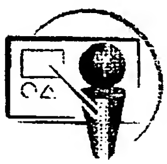
WebEx Services



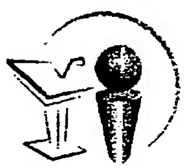
WebEx Enterprise Edition™ enables administrators to provide, and users to access, the complete suite of WebEx interactive services, leveraging the features of the specific service that's best for their needs. WebEx Enterprise Edition is delivered with My WebEx, the personal interface into the WebEx suite of services. Through My WebEx, users within the enterprise can access all of their WebEx services in a single place, with a single login.



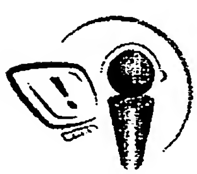
WebEx Meeting Center™ is the most powerful online Web meeting solution available. Users can present, collaborate, demonstrate, sell – anything that can be done in a face-to-face meeting can be done in a WebEx meeting. MediaTone enables productive, online meetings with rich media, using any desktop, laptop, or wireless handheld device.



WebEx Training Center™ empowers users to deliver a rich and compelling live, online classroom experience. Users can maximize the reach, timeliness, and effectiveness of training programs while decreasing delivery costs.



WebEx Event Center™ makes highly effective seminars and exciting multimedia events available with a browser, managed from a user's desktop, all for a fraction of the cost of a traditional enterprise-wide event.



WebEx Support Center™ utilizes the power of WebEx to create a perfect environment for delivering high-quality, low-cost customer support.

Benefits of WebEx Services

Benefits of WebEx services include the ability to share multiple documents and presentations in a meeting and use streaming or local multi-media content. Multiple presenters may collaborate in one meeting, and multi-language meetings are available through a customizable interface. Presenters may run any software application for effective demos, training and team meetings, including applications for:

- Customer relationship management (CRM)
- Enterprise resource planning (ERP)
- Financial management

The following capabilities are included in some or all of the WebEx services:

- Application Sharing
- Remote Control
- White Boarding
- Polling
- Chat
- Q&A
- Breakout Sessions
- Integrated VoIP
- Integrated audio conferencing

Requirements of a Web Communications Platform

Much like the telecommunications infrastructure is built on standards to support voice communications from myriads of endpoints, a Web communications infrastructure must provide for ubiquitous access, allow for an ever-increasing range of functionality, be scalable and extensible, and most importantly be reliable. The Web has been a powerful medium for ubiquitous access to information and services, and a successful communications platform should leverage it for access to its services by individuals who are anywhere in the world and who use any combination of wired or wireless Internet devices. Finally, the infrastructure should provide support for rapid provisioning of an increasing range of services with relatively low cost of ownership.

WebEx Delivers Web Communications Solutions

To meet demand for Web communications services such as online meetings, conferencing, learning and customer support, WebEx is adding live interaction capabilities to the Web. This requires strong support for service management, multi-point conference control as well as robust communications support. Additionally, with full support for sharing any documents including streaming audio and video, Flash, and other rich media formats, WebEx communications services enable users to share applications, take remote control, and interactively annotate on-screen materials. With these services, enterprises have:

- Richer, more effective online communications.
- Faster time to market and quicker problem resolution.
- Lower costs for expenses such as travel, meeting venues and meeting planning.
- Better decision-making.
- Improved productivity and efficiency through the use of real-time interactive Web communications across the enterprise.

Join hundreds of Fortune 1000 companies already using WebEx.
For more information, visit www.webex.com or contact a service consultant at +1.877.50.WEBEX (or +1.408.435.7048).

WebEx History

- Founded, 1996.
- Initial Public Offering, 1999.
- Acquired and developed key technologies in real-time collaboration.
- Today offers a breadth of services that are unparalleled in the industry—plus outstanding scalability, reliability and cost performance.
- Headquartered in San Jose, Calif., with offices in Sacramento, New York, Amsterdam, Melbourne, Hong Kong and Tokyo.
- Approximately 950 employees worldwide.
- Research and Development Centers of Excellence in San Jose, Hangzhou, Suzhou and Hefei.
- Data Centers in San Jose, Denver, Virginia, Hong Kong, Tokyo, Stockholm and London.

Worldwide Sales Offices:

Americas & Canada
Tel: +1.877.50.WEBEX
AmericasInfo@webex.com

Europe, Middle East & Africa
Tel: +31 (0)20.4108.700
EMEAinfo@webex.com

Australia & New Zealand
Tel: +61 (0)3.9653.9581
AsiaPacInfo@webex.com

China (HK)
Tel: +852.8201.0228
AsiaPacInfo@webex.com

Japan
Tel: +81.3.5501.3272
JapanInfo@webex.com

011003.MTWP

Business Solutions/Professional,http://www.accessline.com/business_sol/bs_professional_body.html

Business Solutions / Professional

What if you could:

- Never miss an important call or fax
- Have one, unified voicemail box
- Avoid unwanted calls while only taking the important calls through sophisticated call screening features
- Set up conference calls in less than a minute via the Web or phone
- Give out only one phone number instead of 4 or 5
- Be able to save your voicemails to your hard drive

Let's be honest, you probably have way too many phone numbers. You have your office, home, cellular, fax and maybe even pager number to manage. And remember, you aren't the only one who has to manage all those numbers, you expect your customers, colleagues and family to know which number to call you on and when. With AccessLine SmartNumber, you only give out ONE NUMBER. You then decide which phone to send your callers to. You can also screen calls to make sure you take the calls you want and skip the ones you don't! If you can't take the call, your SmartNumber will take a message.

Also, your SmartNumber is your fax number. SmartNumber automatically knows the difference between someone calling you and an incoming fax. It will store your faxes and let you send them to the fax machine of your choice, or just view them via the Internet.

Simply Log onto AccessLine.com and you can route all your calls to any phone, anywhere, any time. You can view faxes and listen to voicemails right from your web browser and forward them just like e-mails!

In addition to SmartNumber you can also buy other AccessLine products by calling 877-716-2540. Or to try your own AccessLine SmartNumber immediately, click **here to sign up now!**

For more information, please contact:

Justin Bowers, Director of Small Business Sales
jbowers@accessline.com
877-716-2540

"Accessline Comms' Accessline Service, The One-Number Wonder," CommWeb, T. Kramer, February 1, 2000,http://www.cconvergence.com/article/TCM20000504S0014

Comm
fooo
Site Search
search for it
advanced search

Visit these other CommWeb channels

Buyer's Guide | White Papers | Case Studies | Events | Product Reviews | Tutorials | Roundtables | Subscriptions

Current Issue
Past Issues
FAQ
Editorial Calendar
Back Issues
Media Kit
About Us
Contact Us
Teleconnect Archives
Subscriptions

The CommWeb Magazine Network

Call Center
Communications Convergence
Network Magazine

Solutions Center

Buyer's Guide
Product Reviews
Lab Tests
Tutorials
Case Studies

Resource Center

Industry Stats
TechLibrary
TrekMail
Auctions
Chats/Forums
TechEncyclopedia
Subscriptions

Visitors Center

Accessline Comms' Accessline Service

The One-number Wonder.

By Travis Kramer

CommWeb

02/01/2000, 12:00 AM ET

We don't know if this is the direction in which business telecommunications are headed for everyone, or if it's a new trend for itinerant businessmen only, but lately we've been deluged with offers to try out "one-number" services. Accessline Communications (Bellevue, WA - 877-800-0999) approached us with its customizable voice and communications service, AccessLine, an all-in-one number we found perfect for any professional who needs to be in contact with colleagues, clients, and family wherever he goes (and doesn't have a good office voicemail). Accessline will store voice and fax messages, route calls to your current location, host audioconferences, and much more.

THE SETUP

Accessline is easily programmed using a touchtone keypad, and once user-initialized, it's reprogrammable by keypad or the online GUI. You're given a toll-free number and a temporary PIN when you sign up. Since setup for these types of services sometimes entails a delay (a pain when you need to change numbers in a hurry), I set up my Accessline by phone while I logged onto the Web site, and I saw the entered information immediately updated. Accessline (characterized by a friendly female voice) prompts you for your temporary PIN before you record your name and set your own PIN. Once that's accomplished, it's ready for use. When you need to tell Accessline where to forward your calls, you can set your forwarding numbers by phone or online at any time. We were given a handy card containing all the prompt codes we'd need for operating Accessline. The forwarding feature uses two-digit codes to represent the various contact numbers for easy redirection when you call in to change your forwarding options. For example, home is 10, office is 20, cellular is 30, etc. If you're

Utilities

print this article
e-mail this article
license this article

Related Links

Emerging Technology: XML - The End of Security Through Obscurity?

Strategies & Issues: On the Far Side: NAT and Session Border Controllers

Your Rights Don't Need to be Managed

How Far Can 802.11 Really Travel?

Network Innovations That Mattered

Network Address Translation

Strategies & Issues: Measuring End-to-End Internet Performance

Strategies & Issues: Honeypots - Sticking It to Hackers

Zultys Technologies's MX1200 Enterprise Media Exchange

going from home to your office, simply call your Accessline number, enter your PIN, press "2" to direct your calls, and press "20." Two great features for directing calls are the Timer and the Weekly Schedule. If you know how long you'll be near a certain phone, or your schedule demands that you be in the Pennsylvania office every Thursday from 9am til noon, for example, you can set the Accessline timer for the length of time you would like your calls sent to each forwarding number. Enter "*" if you want calls forwarded until further notice, or enter the amount of time (in minutes) that you will be available; then enter the memory number of your next location. Accessline automatically redirects the calls for you. Similarly, the Weekly Schedule automatically directs calls based on your daily or weekly activities, which you enter via the Web. Now your work calls can follow you home on weekends. Wheee!

I'VE GOT MAIL! (VOICE and FAX)

Checking your voice and fax inboxes is a cinch by phone or computer. Voicemail by phone is pretty standard; use the number keys to listen, delete, save, skip, and leave messages. I liked the deletion confirmation feature. After deleting a message, you are prompted to press "5" to confirm deletion or any other key to cancel the action. Superb for countering the caffeine twitchies. We love voicemail features that help you return messages without having to log into and out of your voicemail box; saves time, money, and aggravation. Instant Callback lets you return the call (to any caller who attaches a phone number to a voicemail message) by pressing "9*." The Rebound feature returns you to your voicemail inbox when the call is completed. You also have the option to listen to your voicemail online as a .VOX file (which stores the voice file digitally), save, delete, or even forward messages as email attachments. When checking faxes over the phone, you'll hear the number of new faxes and your delivery options. You can forward faxes in groups (new or delivered) or individually; or choose to send them to your default fax or to an alternate number. Each fax I had delivered arrived almost instantly and came with a cover sheet detailing the date and time received and the sender's fax number. If you're not near a fax machine, you can also view faxes online as .JPG or .TIFF files, or forward them as email attachments. The GUI is convenient and straightforward, working in real time with the touchtone menu.

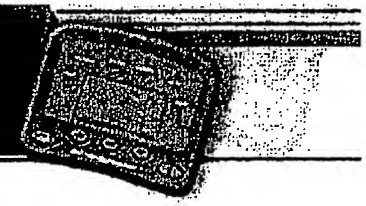
BUT WAIT, THERE'S MORE...

Accessline offers pager notification for incoming calls, voicemail, and faxes. The page for new voice or fax messages displays the appropriate function code, followed by the number of new messages and the calling/faxing party's number. When you get a page for an incoming call on hold, go to any touchtone phone, call your Accessline number, and press "4" to be connected with the call. Call screening is great for hectic days or receiving calls at home; it screens calls based on caller discretion (asks if call is urgent) or your discretion. Accessline also lets you host an inbound conference call using your personal number as the dial-in bridge. You can schedule a conference call (date, time, duration) by phone or online. Participants call Accessline to connect to the conference. Accessline is also testing its Beta release working of an email feature that will configure your POP3 email accounts with your Accessline inbox. Basic service is $18.95/month plus cost of calls (10/min.) and a $40 activation fee.

"InteleScreener," 2003,
http://www.intelescreener.com/howitworks.html

InTele creener™

A Revolution in Telephone Privacy



Phone Orders Call
1-866-884-9524

- Home
- Order Yours Today!
- Registration Form

Product Information

- How It Works
- Features
- Applications
- Operating Manual
- FAQs
- Glossary

Company Information

How InTeleScreener Works

The **InTeleScreener**™ works with your telephone company's Caller ID service. Caller ID information is sent between the first and second ring on an incoming phone call. The **InTeleScreener**™ blocks the first ring from ringing the telephone and processes the Caller ID information to screen the phone call prior to the second ring. Depending on the mode of operation the call will either be blocked or allowed to ring your telephone.

Block Mode

During block mode, any incoming calls from a number that is in the block list, the **InTeleScreener**™ will block them from ringing the telephone. Callers not in the block list will be allowed through to ring your phone. Numbers can be added to the block list simply by pressing BLOCK while viewing the Caller ID display or later while reviewing the history list.

The **InTeleScreener**™ has the two following options for blocking callers in the block list, both of which never allow your telephone to ring:

Block Mode: Disconnect Call
This option will answer the call, emit the disconnect (SIT) tones to the caller making your phone look like it has been disconnected and then hang-up. This is all done automatically by the **InTeleScreener**™ without allowing the telephone to ring and disrupt you.

Block Mode: Do Not Answer
This option will prevent your phone from ringing, but will not disconnect them or emit the disconnect tones. To the caller it will appear as if your phone is ringing and you are not answering. Use this option when you do not want to disconnect the caller or want to allow caller to leave a voice message. It is also useful when you have multiple **InTeleScreener**™ devices and wish to block a phone call in one room while allowing the call to ring another telephone in a separate room. This mode is useful for teenagers or if you live with roommates and do not want people

calling for them to ring your phone.

Screen Mode
In Screen mode your phone will only ring when the call is from someone in the Screen List such as family and friends. Screen mode allows you to choose who can ring your phone. Numbers can be added to the screen list simply by pressing SCREEN while viewing the Caller ID display or later while reviewing the history list. No more wrong numbers in the middle of the night or telemarketers bothering you during a quiet dinner.

Auto Mode
The **InTeleScreener™** is fully programmable so the user can customize it to his/her lifestyle. Auto mode allows the user to program the **InTeleScreener™** to run Block and/or Screen mode during preset time periods throughout the day or night. Whether you sleep during the day or night you will be able to sleep peacefully while the **InTeleScreener™** screens all of your phone calls.

Consumers more than ever are wanting to stop telemarketers from calling and disrupting their privacy. Traditional call block services from telephone companies used to block telemarketing calls are costly and ineffective at stopping telemarketers from calling. Many phone companies offer anonymous phone call screening services to stop telemarketers and unknown callers requiring them to un-block caller ID or identify themselves before they can ring through. The InTeleScreener was invented not only to block telemarketers but to give the consumer the best available product ever for stopping telemarketers from calling and all other unwanted callers from ever ringing their phone. If you want the best Caller ID device to block telemarketers and you want unbeatable phone call screening to finally stop telemarketers, you need to get the InTeleScreener Caller ID today. Stop paying for expensive call block services from your phone company and get the InTeleScreener to finally stop telemarketers from calling and disrupting your privacy.

Order online today or call us toll free ***1-866-884-9524***

"TeleZapper from Privacy Technologies," Privacy Corps - Our Review, 2002,http://www.privacycorps.com/pages/product1.htm

Privacy Corps

Fighting For Your Privacy

STARTLING STATISTICS

Charities make more money from *selling your name and number* to the other telemarketing companies than from the donations they collect from calling.

REFER A FRIEND to Privacy Corps

Your Email:

Their Email:

send

TeleZapper from Privacy Technologies

Our Review

Under real test conditions, on average, the number of telemarketing calls per test site was reduced from two telemarketing calls a day to approximately two calls per month, over a period of four weeks. We found these test results pretty darned good!

The TeleZapper was incredibly easy to connect using the simple diagrams provided. The telephone cords connect in two places, one into the TeleZapper from the telephone-company line and one out of the TeleZapper to your telephone. All you have to do is unplug the line to your phone and connect the TeleZapper in its place. A connection cord is also provided to connect the TeleZapper to the wall jack. You'll need to plug the Telezpapper into an outlet to power the TeleZapper unit, but the manufacturers have provided a plug and cord.

Once connected, the TeleZapper works in the background and requires no further input from the user. You'll only need one TeleZapper for all phones connected to that line. However, if you have more than one telephone number, you'll need a TeleZapper for each additional phone line.

The tone transmitted when the telephone is answered is very short and subtle, and testers report that most callers don't even hear it. If they do notice it, generally the comments came from callers after their third or forth call, but most didn't feel that it was at all intrusive.

We also tested the product with the company phone system which has it's own control unit, intercom, and multiple phones. The TeleZapper worked just as well under these conditions, although because our business uses several lines, we needed several additional TeleZappers.

As an added benefit, the TeleZapper continues to work in the background even when

an answering machine picks up the phone, resulting in a diminished number of calls over time. The calls that did get past the TeleZapper were manually dialed calls from smaller, more local companies, dialing numbers for each area in sequence.

Privacy Corps recommends this product as a good value, in terms of ease of use, effectiveness, and reliability. We were also pleasantly surprised by the free technical support available from the manufacturer via their toll-free number.

Purchase Now!

Customer Testimonials

Just wanted to let you know I bought the TeleZapper out of desperation a few weeks ago. My home telemarketing calls have now STOPPED!!! THANK YOU SO MUCH! You have saved my sanity. *Sue - Manassas, VA*

Thank you, TeleZapper! You've saved me the cost of replacing the glass in my bedroom window, and a doctor bill for trying to throw my phone a hundred yards! Yes, I'm talking about those late, and I do mean late, nighttime calls trying to sell me everyting from newspapers, family portraits, to life insurance! Ah, privacy...what a beautiful word! *Ruben - Palmdale, CA*

We would love to hear from you if you have used one of our products!

CLICK HERE to fill out our product feedback form.

Frequently Asked Questions (FAQ)

- How do telemarketing calls work?
- How does my number get on telemarketing lists?
- How does the TeleZapper "zap" telemarketers?
- Will the TeleZapper "zap" calls from anyone other than telemarketers?

How do telemarketing calls work?

There are several hundred telemarketing call centers in the U.S., with the vast majority of telemarketing calls being dialed by a computer known as an auto dialer or predictive dialer. Predictive dialers can dial 3-5 numbers simultaneously and can make as many as 500,000 calls between 8 a.m. and 9 p.m. When you answer your phone, the computer connects you to a live telemarketer who tries to sell you something. If you are not home or if the computer gets your answering machine, your number will be put back in the database to be called again later.

Back to top...

How does my number get on telemarketing lists?

You can get on telemarketing lists in many ways:

- By having a listed telephone number;
- Through a reverse phone book organized by neighborhood;
- When you dial an 800 number that uses an Automatic Number Identification system (ANI) to record your number;
- Via credit information services, such as Equifax, etc.;

- By ordering products or services from direct marketers or catalogs, whether you order through the mail, from web sites, or via 800 numbers;
- By printing or including your telephone number on your personal checks;
- Even by simply paying your monthly bills.

These lists of telephone numbers are then often sold, bartered, rented, shared and copied from one telemarketer to another. As your number constantly finds its way onto new call lists, the TeleZapper will continue to do its job over time to help you protect your privacy.

Back to top...

How does the TeleZapper "zap" telemarketers?

The TeleZapper uses the technology of telemarketers' automatic dialing equipment against them. When you or your answering machine picks up a call, the TeleZapper emits a special tone that "fools" the computer into thinking your number is disconnected. When the computer hears the tone, it hangs up before you can be connected to a telemarketer and then deletes your phone number from its database. Overtime, as your number is removed from more and more databases, you'll see a dramatic decrease in the number of annoying telemarketing calls you receive.

Back to top...

Will the TeleZapper "zap" calls from anyone other than telemarketers?

The TeleZapper is designed to "zap" calls made by predictive dialer computers by doing two things: first, by disconnecting predictive-dialed calls before you can be connected to a live telemarketer and second, by deleting your phone number from telemarketing computer lists. Whether the TeleZapper will affect computer-dialed calls from other sources depends on the type of computer equipment and how that equipment is being used. Therefore, it may also "zap" calls from other organizations that use predictive dialer computers, such as charitable organizations, blood banks, public safety and service organizations, market researchers, opinion and political pollsters, and academic institutions.

Many organizations and communities do not rely entirely on computerized calling systems to reach you. Most have secondary means in place to contact or notify people with important information. Furthermore, these organizations can always contact you by simply dialing your phone number manually. Manually dialed calls will not be zapped. As such, you can notify organizations to determine if they use predictive dialers and, if so, to ask that your phone number be manually dialed or that alternate means be used in order to contact you.

Finally, during times of severe weather or at any time that important public emergency notifications might be received, you can quickly and easily disconnect your TeleZapper to allow all calls, including those placed by computerized dialers, to be successfully completed.

Back to top...

How do I know when I've "zapped" someone?

If you answer your telephone and there's no one there, the odds are that you just "zapped" a telemarketer. After a few weeks, you'll notice that you are receiving fewer and fewer of these calls.

Back to top...

Why buy a TeleZapper instead of letting my answering machine or caller ID screen telemarketing calls?

The TeleZapper is the only product that emits a signal that "tells" predictive dialer computers your number is disconnected. Unlike answering machines or caller ID, once the TeleZapper's tone is emitted, your number is removed from the computer's call list. So, as time passes, you'll receive fewer and fewer annoying telemarketing calls. If the computer gets your answering machine, your number is put back into the database to be called again and again ... and again. Most telemarketing calls show up on Caller ID as "out of area" or "private". But since many callers are identified in these ways, it's difficult to know who's calling and whether or not you want to pick up the phone. The TeleZapper really is a better solution to keep telemarketers out!

Back to top...

How do I install the TeleZapper?

The TeleZapper is easy to install. Simply plug it into any electrical outlet and phone jack to cover all extensions and answering machines connected to that line. Plus, you have flexibility to place the TeleZapper anywhere in your home since you can plug the phone cord into a phone, into an answering machine, or directly into a phone jack.

Back to top...

Do I need a TeleZapper for each telephone extension?

No. One TeleZapper covers all telephones and answering machines connected to the same line (telephone number). If you have two lines, you will need an additional TeleZapper for your other line.

Back to top...

Do I need to use a special phone with the TeleZapper?

No. The TeleZapper works on any home phone line and with any type of phone.

Back to top...

Will the TeleZapper interfere with my answering machine?

No. The TeleZapper will not interfere with your answering machine. In fact, the TeleZapper works with your answering machine to "zap" telemarketers when you are away or when you prefer not to answer the phone. When your answering machine picks up a call for you, the TeleZapper emits its special tone to "zap" the telemarketer. Your name will have been deleted from another telemarketing list and you won't have been bothered at all. We do recommend that you re-record your message and delay speaking for a few seconds to allow time for the TeleZapper tone prior to the start of your recorded message. A caller who wishes to leave a message on your answering machine will hear a short tone followed by your recording.

Back to top...

I have voicemail from the telephone company. Will the TeleZapper work with this?

Yes and No. Your telephone must go "off-hook" for the TeleZapper to emit its tone. As long as you pick up a call, the phone goes "off-hook" and the TeleZapper emits its tone to "zap" telemarketers. If, instead, the telephone company "answers" your calls through voicemail, your phone does not go "off-hook" and the TeleZapper cannot emit its tone. The TeleZapper will not interfere with the normal operation of your voicemail.

Back to top...

Will the TeleZapper interfere with my computer or fax machine?

No. The TeleZapper does not interfere with the operation of your computer, your fax machine or other telecommunications or electronics equipment.

Back to top...

Will the TeleZapper work on junk faxes?

Yes. If your fax number is dialed by a computerized predictive dialing system that is programmed to listen for disconnected numbers, the TeleZapper will "zap" your fax number from those calling lists.

Back to top...

When is/should the red LED light on the TeleZapper be on?

The red LED light flashes three times when the phone is picked up and the TeleZapper emits its tone. Since the light is off at all other times, it does not mean your TeleZapper is not working when the light is not illuminated.

Back to top...

What's to keep telemarketers from just turning off the "disconnected" feature on their computerized dialing equipment?

Plenty! There are millions of non-working telephone numbers. Telemarketers succeed by efficiently connecting their operators to PEOPLE and then selling them something. The last thing they want is to waste time being connected to a non-working telephone number. Plus, when you've installed a Telezapper, you're telling the telemarketer you do not want to talk to them. There are laws that support your right to privacy and most telemarketers really don't want to violate those laws -- they just want to talk to someone who might buy something.

Back to top...

Does the TeleZapper block collectors' computer generated calls made to collect legitimate debts?

By purchasing the TeleZapper, you are making a choice to protect your privacy. Before the introduction of the TeleZapper, you may have used other methods to screen unwanted calls, such as Caller ID, Privacy Manager, and answering machines. The TeleZapper is simply another option for people who are concerned about maintaining their privacy. That right is a fundamental one and is, indeed, constitutionally protected.

The vast majority of telemarketing calls are computer dialed at random. The TeleZapper is designed to "zap" your phone number off telemarketers' computers. Whether the TeleZapper will affect computer-dialed calls from other sources, such as collection agencies, depends on the type of computer equipment being used and how that equipment is being used. Therefore, the TeleZapper may also "zap" calls from organizations, other than telemarketers, that also use predictive dialer computers.

The TeleZapper will not "zap" bill collectors or other companies who dial a telephone number manually rather than through a predictive dialing computer.

Back to top...

Does the TeleZapper block incoming calling card calls?

Telezapper has learned that some long distance calling card manufacturers use a system similar to predictive dialing systems. Whether the TeleZapper will affect computer dialed calling card calls depends on the type of computer equipment and how that equipment is being used. Since the TeleZapper is designed to disconnect calls before a computerized predictive dialer can connect you to a live telemarketer/caller, there is also a chance that predictive-dialed calling card calls may not be completed.

Back to top...

Does the TeleZapper create a computer virus for the caller?

The TeleZapper DOES NOT create a computer virus for callers. The TeleZapper simply emits a tone that predictive dialer computers recognize as a disconnected number.

Back to top...

Does the TeleZapper interfere with a DSL connection?

The TeleZapper DOES NOT interfere with a DSL connection. Be sure that the Telezapper is connected at a point after the DSL junction box.

Back to top...

What are the differences between the TeleZappper and TeleZapper II?

Besides being smaller in size the TeleZapper II offers a user-selectable switch to choose between emitting one or three tones. It is also powered by a lithium battery with a projected useful life of approximately 7 years, and does not require household current.

Back to top...

Home | About Us | Products | Newsletter | Resources | Affiliate Program | Contact Us | Site Map

Privacy Statement | Terms of Service

"A Proposal for Internet Call Waiting Service Using SIP," A. Brusilovsky et al., Lucent Technologies, PINT Working Group, Internet Draft, January 1999.

PINT Working Group
Internet Draft

A. Brusilovsky
E. Gausmann
V. Gurbani
A. Jain
Lucent Technologies

Expires: July 1999

A Proposal for Internet Call Waiting Service using SIP
An Implementation Report

<draft-brusilovsky-icw-00.txt>

Status of this Memo

Abstract

The purpose of this Internet Draft is to start discussion on the issues involved in Internet Call Waiting Service (ICW), as part of interconnecting IP and Global Switched Telephone Network (GSTN) with the intent of providing ICW service that is much needed by numerous dial-up Internet users. Interworking of the IP network and GSTN, based on open well-defined protocols, will promote interoperability of both the networks and systems built by different vendors. This Internet Draft is submitted with the goal of becoming an informational RFC.

The rest of this document is as follows:

Section 2 briefly describes the services offered to the end Subscriber. It is the support of these services that necessitates the proposed internetworking project.

Section 3 describes the scope of the proposed project by introducing its overall architecture, identifying the interfaces to be standardized, describing experience with SIP for ICW.

Sections 4, 5, and 6 respectively address security considerations, supply references, and provide the authors address, as required by [1].

Section 7 acknowledges individuals providing assistance in the creation of this document.

Section 8 is the Appendix, which contains IN Tutorial and Figure A.

2. Service Description

It is a well-known problem that call waiting tone interferes with the operation of a modem. Anyone using the telephone for a modem connection to a host computer can not gracefully deal with incoming call waiting calls. Internet Call Waiting is the capability to provide incoming call notification and completion options when the Subscriber is on a dial-up IP connection. When a call comes in the Subscriber is presented with a pop-up dialog box, that presents the caller's number and, optionally, his or her name. Internet Call Waiting solution provides a simple, graphical-oriented way to notify subscribers while connected to the Internet, of incoming calls. It allows the subscriber to accept or reject the call.

Benefits

Service providers can achieve the following important benefits through the use of Internet Call Waiting Service:

o More calls completed. Call completion is an important aspect of the service provided by telecommunication operators. Calls that end in busy or no- answer, consume network resources. Solution like Internet Call Waiting contributes to greater call completion which lowers expense and provides value to both the consumer and service provider.

o The ICW platform is the foundation to offer services: The service provider has the opportunity to enhance Internet Call Waiting with other services like Internet Follow-me, personalized call management, unified messaging service, click to return (dial) an important call, and other call management functions which integrate voice and data services.

o Service provider can offer the following important benefits to the subscribers through the use Internet Call Waiting Service:

- Simple way to manage voice and data calls over a single telephone line.
- Ability to track all incoming calls while the service is active
- PC Graphical Subscriber Interface provides a simple intuitive Subscriber interface and also allows easy customization.

3. Scope of the Proposed Project

Figure A illustrates the hardware architecture that will support ICW Service. The lines indicate the control and/or voice paths. Control paths are labeled by the protocol that will be used over them.
IN elements (SCP, SMS, SSP) are specialized servers, connected to switches and other network elements. They handle data queries and updates, specialized call routing and other advanced telecom services. For more information on Intelligent Network please see our IN Tutorial in the Appendix of this Internet Draft.

The following software components make up the ICW architecture.

o ICW User Agent Server (UAS) - The ICW UAS (SIP Client) and server communicate via the SIP protocol over TCP/IP. The ICW UAS can start up automatically as soon as a PPP connection is established. It also responds to the incoming request for call treatment by popping up the dialog box to the subscriber presenting information about the Calling Party and asking for an Accept or Reject decision. The UAS sends the resulting choice back to the ICW server. In the case of a accepted call, the UAS drops the modem connection to the ISP to allow the incoming call to complete.

o ICW server - a SIP proxy server that perform the following

functions. The SCP is not being used as a general-purpose database host. Thus, SIP-related database dips are envisioned to be in the domain of a generic ICW server which can interface with any commercial-grade database engine or any LDAP-enabled database. The SCP is free to provide telecommunication intensive tasks that it was designed for.

- Listening for incoming messages from the application running on SCP
- Providing a data store mechanism for ICW applications
- Handling Web-based GUI (Applet) requests for subscriber provisioning on the ICW server

o SCP platform software - The ICW APPLICATION runs on SCP

- ICW Application runs on SCP - The AIN 0.1 Terminating Attempt Trigger (TAT) is used to enable PSTN call handling. Thus, the Application responds to an AIN message for every call to the subscriber. For each call, the Application either returns a request for normal routing, if the subscriber is no longer active,

or sends a message to the ICW server passing along the calling number. Based upon the reply from the ICW server, which may be Accepted or Rejected, the SCP sends the appropriate instructions ba ck to the SSP.

Various alternatives exist for firewall support. The ICW UAS-to-ICW server firewall could be standard corporate security firewall. However, the security policy would need to allow TCP-based SIP messages to flow between the ICW UAS and server over the standard SIP port 5060. The ICW server-to-SCP firewall is optional and could be used to provide an extra level of protection for the SCP by restricting Intranet access or by enforcing a more restrictive security policy than the outer firewall. General and ICW specific security considerations are covered in Section 4.

Other components in the diagram are part of the standard Internet and PSTN and include the Internet Service Provider (ISP), ISP modems and web servers, the Service Switching Point (SSP) and the Signal Transfer Point (STP). The SSPs must be provisioned with the necessary trigger for the ICW service, the AIN 0.1 Terminating Attempt Trigger.

When the Calling Party dials the ICW Subscriber's Destination Number, the Calling Party experiences the standard Call Waiting treatment, ringing, until Calling Party abandons or the Subscriber specifies treatment: Subscriber treatment options and Calling Party experience are:
o Refuse Call: Calling Party hears ringing until Calling Party abandons. In SIP terms, this results in the SIP UAS sending a "603 Decline" message to the ICW server.
o Hold Call: Calling Party hears [optional] announcement to hold while "other" call in progress is completed. The intent is that the Subscriber will accept the call momentarily. (Another possibility would be to tell the Calling Party that you'll call them back in a few minutes, etc) In SIP terms, this results in the SIP UAS sending a "182 Queued" message to the ICW server.
o Send to Voice Mail (assuming Subscriber has a Voice Mail service): Calling Party hears voice mail system announcements. (This redirection to voice mail could, as well, have been redirection to some other DN, e.g. cell phone, second line, secretary, etc) In SIP terms, this results in the SIP UAS sending a "380 Alternative Service" to the ICW server.
o Accept Call: Calling Party hears ringing until is connected to Subscriber. In SIP terms, this results in the SIP UAS sending a "200 OK" to the ICW server.
Note: Optional treatment options can include taking call via VoIP and route call to a third party number.

In the proposed Architecture, the Subscriber is assumed to have PPP service through their ISP. They are surfing the Internet or working at home, connected to a corporate intranet. Two components of ICW

reside on their PC; an H.323 client for VoIP and an ICW UAS to drive the presentation to the Subscriber of Setup and Notification. Controlling the ICW service is the ICW server for Internet related control and the combination of the SCP and SSP via AIN functionality providing PSTN control via SS7. There is an ICW control session between the PC and the ICW server. Controlling the VoIP aspect is the H.323 client at the PC and the H.323 gateway with H.323 packets going between them via the internet. The SCP controls the IP via Bellcore's GR-1129. The SCP and ICW server have a TCP/IP connection. The call path of the accepted call consists of the Calling Party being routed to the IP (intelligent peripheral) and bridged to the ICW Subscriber from the H.323 gateway. Firewall appliances are placed on all IP connections of the service provider. A call scenario below walks through this architecture. Integration of the H.323 GW and IP as well as the SCP and ICW server is a possibility for future enhancements.

Call Scenario

Subscription to the service.
o Subscriber signs up for the service.
o Subscriber downloads and installs the ICW UAS software.
o Subscriber Information is provisioned in the SMS (and SCP).

Activation of the service and coordination with the ICW Server (Transparent for the ICW User)
o ICW UAS establishes TCP connection.
o Subscriber authenticates himself/herself and Register with ICW Server using the encrypted password and phone number.
o ICW Server stores information in database.

Call Arrival
o Calling Party initiates call to Subscriber.
o SSP (Switch) encounters TAT.
o SCP query launched.
o SCP determines if call is for an ICW subscriber (if not then other service logic applies).
o SCP sends a SIP "INVITE" message with Calling Number, optional Calling Name and Called Number (and receives a SIP acknowledgement from the ICW Server)
o If ICW is activated for the called subscriber, ICW Server returns "TRYING" to SCP. The SCP instructs SSP to play an announcment, e.g. ringing. ICW Server determines, based on the Called Number and the IP Address of the ICW UAS and sends the SIP INVITE message to the ICW UAS.
o If ICW is not activated ICW Server returns "NOT FOUND" to SCP. SCP returns an Authorize Term message to the SSP so call proceeds as normal.

Communicating subscriber's choice to the SCP.
o ICW UAS returns a SIP "DECLINE" (for normal SSP treatment) or "OK"

(for connecting the call).
o ICW Server passes along the SIP message to the SCP

Choice: Drop Modem, take call.
o ICW UAS causes Modem to drop.
o SCP instructs switch to continue with the call (Authorize Term).
o Switch connects Calling Party to Subscriber line causing the phone

to ring.

Choice: Send to Voice Mail.
o SCP sends Authorize Term message to switch to deliver the call to the subscriber's line.
o SSP detects Busy and uses standard Call Forwarding on Busy to send to Voice Mail

Experiences in using SIP for ICW Project

The biggest advantage to using SIP in the ICW project was its ASCII-based nature and a concise set of messages. We were able to get a bare-bones SIP server running in a good part of a week. SIP is geared towards Internet protocol services; ICW is a prime example of such a service. SIP's semantics lend themselves very efficiently to the semantics of the ICW service. SIP has a very rich set of response codes that we were able to tailor to the various ICW states, such as the user accepting a call, declining a call, redirecting a call to a new location, or simply not being on the PC when the call notification arrived. Another advantage of SIP is that a SIP-based architecture is easily explained to even those who do not possess an in-depth understanding of Internet in general and IP protocols in particular. Various SIP entities like SIP User Agent Server, Proxy Server, Redirect Server, etc. lend themselves to a very extensible architecture.

The disadvantages of SIP are few; one of them being its constant state of flux. During ICW development, the SIP draft RFC changed no less then 3 minor versions. This made it somewhat difficult to agree on a standard. However, this disadvantage will be mitigated in the future when the SIP draft becomes a Draft Standard. The other big disadvantage was driven by the general lack of support for database queries. For instance, an SCP would like to authoritatively know if a user was on the Internet before sending him/her the call notification. However, the SIP message set did not support general querying capabilities for this purpose. We ended up using the SIP OPTIONS message for this purpose, even though the draft mandates that OPTIONS message is used primarily for capability set negotiations. Finally, the SIP RFCs are becoming more complex with each new revision. We believe that while adding features is critical, it would be in the best interest to maintain the simplicity of SIP for rapid development, debugging, and deployment.

Security Considerations

ICW communications between the PC and the ICW Server may travel over the Internet. Thus it is essential to provide encryption for the communications. In addition to encryption, and to make sure that the PC belongs to a registered subscriber, it is also necessary to provide authentication of both the end points; i.e. ICW Server and the PC. ICW security has been designed to authenticate both end points and if the authentication succeeded, encrypt the communications (control channel) using a symmetric key. This key is provisioned in the ICW Server database as well as generated at the subscriber's end-point (the PC) when the software is initially installed. In the future, migration of the ICW security infrastructure to SSL is envisioned.

ICW Security Requirements are, assentially, the same as PINT Security Requirements outlined in [4]:

o Peer entity authentication to allow a communicating entity to prove its identity to another in the network. Two types of peers should be recognized for the purposes of this project: end-user and the Web server, and Web server and SN. Between the end-user and Web server the authentication could be accomplished by means of the user name and password combination. In addition, encrypted communications could be used in this case. Same could be used between the Web

server and SN, but it is proposed that additional security be accomplished by replicating a part of the server's data base relevant to the business providing the service.

o Non-repudiation to account for all operations in case of doubt or dispute. This could be achieved by logging all the information pertinent to the Web transaction. In addition, the PSTN network will maintain its own account of the transaction for generating bills.

o Confidentiality to avoid disclosure of information without the permission of its owner. Although this is an essential requirement, it is not particular to the proposed project.

o End-user profile verification to verify if the end user is authorised to use a service.

In the course of the project execution, additional requirements are likely to arise and many more specific security work items are likely to be proposed and implemented.

Some of the ICW-specific security considerations:
o Hacking is a threat to any Service Provider (PSTN, Intranet, Internet). It is real danger - phone companies are common targets
o Strong Firewall solutions are needed
o Fraudulent Subscription is one of the threats
o Existing mechanisms applied to the Internet can be implemented
o Stealing a Call is a new type of security threat

o Denial of telephone service attack is possible
o Encrypted password protection can be used as one of the possible solutions.

5. References

[1] J. Postel, RFC 1543, "Instruction to RFC Authors". October 1993

[2] ITU-T Q.12xx Recommendation Series, Geneva, 1995.

[3] I. Faynberg, L. R. Gabuzda, M. P. Kaplan, and N. J. Shah, "The Intelligent Network Standards, their Application to Services". McGraw-Hill, 1996.

[4] M. Krishnaswamy, "PSTN-Internet Internetworking - An Architecture Overview", Internet Draft

[5] H. Schulzrinne, "SIP for Click-To-Dial-Back and Third-Party Control", Internet Draft

[6] S. Petrack, "IP Access to PSTN Services: Basic Service Requirements, Definitions, and Architecture", Internet Draft

[7] Handley, Schulzrinne, Schooler, Rosenberg, "SIP: Session Initiation Protocol", Internet Draft

6. Authors' Address

Alec Brusilovsky
E-mail: abrusilovsky@lucent.com
Telephone: +1-630-713-8401
Fax: +1-630-713-5840
Lucent Technologies
263 Shuman Blvd.
Naperville, IL 60566 USA

Eric Gausmann
E-mail: egausmann@lucent.com
Telephone: +1-630-713-5361
Fax: +1-630-713-5840

Lucent Technologies
263 Shuman Blvd.
Naperville, IL 60566 USA

Vijay Gurbani
E-mail: vkg@lucent.com
Telephone: +1-630-224-0216
Fax: +1-630-713-5840
Lucent Technologies
263 Shuman Blvd.

Naperville, IL 60566 USA

Ajay Jain
E-mail: ajayjain@lucent.com
Telephone: +1-630-979-5218
Fax: +1-630-713-5840
Lucent Technologies
263 Shuman Blvd.
Naperville, IL 60566 USA

Glossary

AIN	Advanced Intelligent Network
API	Application Program Interface
DN	Destination Number
GSTN	Global Switched Telephone Network
ICW	Internet Call Waiting
IN	Intelligent Network
IP	Intelligent Peripheral
PSTN	Public Switched Telephone Network
POTS	Plain Old Telephone Service
SCP	Service Control Point
SIP	Session Initiation Protocol
SN	Service Node
SMS	Service Management System
TAT	Terminating Attempt Trigger
UAS	User Agent Server (SIP Terminology)
VoIP	Voice over IP (Internet Protocol)

7. Acknowledgments

The authors would like to acknowledge Igor Faynberg, Jenny Huang, Jack Kozik, Hui-Lan Lu, Bill Opdyke, Jonathan Rosenberg, Henry Sinnreich, Doug Varney and Kumar Vemuri for their insightful comments presented at the working discussions that lead to the creation of this document. Our special thank you is going to John Stanaway for being instrumental in utilizing SIP for the ICW project.

8. Appendix (IN Tutorial and Figure A)

Intelligent Network (IN), excerpt from [4]

IN ([2], [3]) is an architectural concept that provides for the real-time execution of network services and customer applications in a distributed environment consisting of interconnected computers and switching systems. Also included in the scope of IN are systems and technologies required for the creation and management of services in this distributed environment.

In PSTNs, user's telephone terminals and fax machines are connected to telephone switches. The switches (which can be Central Offices--for wireline communications and Mobile Switching Centers (MSCs)--for wireless communications) are specialized computers engineered for provision of services to the users. The switches themselves are interconnected in two ways: 1) through trunks on which the voice is carried and 2) through a specialized fault-tolerant data communications network, which is (principally) used for call setup and maintenance. This network is called (after the ITU-T standard protocol suite that it uses) Signalling System No. 7 (SS7). In addition, the switches are connected to general purpose computers that support specialized applications (called Operations Systems) whose role includes network management, administrative functions (e.g., billing), maintenance, etc. Operation systems are not connected to the switches through the SS7 network, which is, again, engineered only for set-up and real time maintenance of calls. In most cases, X.25 protocol is used for communications between operations systems and switches. Even a simple two-party call in most cases involves several switches, which may also be located in different PSTNs. To this end, the switches alone comprise a complex distributed processing environment. As far as the end users are concerned, the switches are ultimately responsible for delivering telecommunications services. Certain elementary services (such as provision of the dial tone, ringing the called line, and establishing a connection between two users) are called basic services, and all switches can presently cooperate in delivering them to end users.

In addition, a multitude of services (such as Freephone [a.k.a. 800 number in North America], Conference Calling, Call Forwarding, and many others) require much more than basic call processing. Such services are called Supplementary Services, and their implementation requires that specialized applications (called Service Logic) be developed. Developing switch-based service logic for each supplementary service would be an extremely expensive (if at all possible) task, which--in the presence of multiple switch vendors--would also require an extensive standardization effort.

The IN architecture is the alternative which, in a nutshell, postulates using a network-wide server (called Service Control Function [SCF]). The SCF executes service logic and instructs the switches on how to complete the call. A switch is involved only in executing the basic call process, which is interrupted (at standardized breakpoints called triggers) when specialized service logic needs be executed. On encountering such a breakpoint, the switch issues a query to the SCF and waits for its instruction. In addition (and this is essential for supporting the services described in section 2), the SCF may initiate a call on its own by instructing switches to establish necessary connections among themselves and to the call parties.

Physically, the SCF may be located in either stand-alone general purpose computers called Service Control Points (SCPs) or specialized pieces of equipment called Service Nodes (SNs). In addition to executing service logic, a service node can perform certain switching functions (such as bridging of calls)as well as a set of specialized functions (such as playing announcements, voice recognition and text-to-speech conversion). An important distinction between an SCP and SN is that the former is connected to switches via the SS7 network while the latter communicates with the switch via Integrated Services Digital Network (ISDN) Primary or Basic Rate Interfaces (PRI or BRI), which combine both the signaling and voice paths. With the present state of IN standardization, in principle, either an SCP or SN could be connected to an Internet server in order to support the services outlined in section two. To further narrow the scope of work so as to produce tangible results as soon as possible, the proposed project specifically addresses only interconnection between a server and SN.

Within the IN architecture, the relevant administration of the network entities (i.e., setting the triggers in the switches, transferring externally developed service logic to SCPs and SNs, and maintaining the network databases with the customer-related data) is performed by a specialize Operation System called Service Management System (SMS).

Figure A

```
                                                    |F|
                                                    |i|
+---------------------+         =============       |r|
|            +-------+|         ||          ||  SIP |e|     +---------+
| PC Access  |  ICW  ||         || Internet |+-..-..|w|-..-..-| ICW    |
| o..........+  UAS  ||         ||          ||      |a|     | Server |
|            +--+----+|         =========+===       |l|     +---+-----+
| Voice Access :      |                  |          |l|         |
| O------------I:     |                  :                 _____:_____
|              I:     |                  | SIP              Firewall
|              I:     |                  :                 -----------
|              I:     |                  |                      |
|              I:     |              +---+---+                  :
|              I:     |              |  ISP  |                  |
|ICW           I:     |              +---+---+                  :
|Subscriber    I:     |                  |          +--------+  +---+---+
+--------------I:-----+     PPP          :          |  SMS   |---|  SCP  |
               I:......................+ |          +--------+  +---+---+
               L----------------------+: :                          s
                  POTS          =======I:=|==========                |
                               ||      I: :          ||         ====s====
                               ||      I: |          ||         ||      ||
                               ||      +++-+---+     ||         || SS7  ||
  o----------------------------++------|  SSP  |     ||         ||Network||
Calling Party                  ||      +---+---+     ||         =====s====
(Voice Access)                 ||        s P S T N   ||              |
                               ========= | =========       SS7      s
                                         s-s-s-s-s-s-s-s-s-s-s-s-s+
                                                 Signaling
  Legend:
  ..-..- - SIP (over IP)
  s-s-s  - SS7 signaling links
  -----  - POTS connection
  .....  - PPP connection
```

"A Model for Presence and Instant Messaging", M. Day, et al. Fujitsu, February 2000, Network Working Group, Request for Comments 2778.

Network Working Group
Request for Comments: 2778
Category: Informational

M. Day
Lotus
J. Rosenberg
dynamicsoft
H. Sugano
Fujitsu
February 2000

A Model for Presence and Instant Messaging

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This document defines an abstract model for a presence and instant messaging system. It defines the various entities involved, defines terminology, and outlines the services provided by the system. The goal is to provide a common vocabulary for further work on requirements for protocols and markup for presence and instant messaging.

1. Introduction

A presence and instant messaging system allows users to subscribe to each other and be notified of changes in state, and for users to send each other short instant messages. To facilitate development of a suite of protocols to provide this service, we believe that it is valuable to first develop a model for the system. The model consists of the various entities involved, descriptions of the basic functions they provide, and most importantly, definition of a vocabulary which can be used to facilitate discussion.

We note that the purpose of this model is to be descriptive and universal: we want the model to map reasonably onto all of the systems that are informally described as presence or instant messaging systems. The model is not intended to be prescriptive or achieve interoperability: an element that appears in the model will not necessarily be an element of an interoperable protocol, and may not even be a good idea.

In this document, each element of the model appears in upper case (e.g., PRESENCE SERVICE). No term in lower case or mixed case is intended to be a term of the model.

The first part of this document is intended as an overview of the model. The overview includes diagrams, and terms are presented in an order that is intended to help the reader understand the relationship

between elements. The second part of the document is the actual definition of the model, with terms presented in alphabetical order for ease of reference.

The overview is intended to be helpful but is not definitive; it may contain inadvertent differences from the definitions in the model. For any such difference, the definition(s) in the model are taken to be correct, rather than the explanation(s) in the overview.

2. Overview

The model is intended to provide a means for understanding, comparing, and describing systems that support the services typically referred to as presence and instant messaging. It consists of a number of named entities that appear, in some form, in existing systems. No actual implementation is likely to have every entity of the model as a distinct part. Instead, there will almost always be parts of the implementation that embody two or more entities of the model. However, different implementations may combine entities in different ways.

The model defines two services: a PRESENCE SERVICE and an INSTANT MESSAGE SERVICE. The PRESENCE SERVICE serves to accept information, store it, and distribute it. The information stored is (unsurprisingly) PRESENCE INFORMATION. The INSTANT MESSAGE SERVICE. serves to accept and deliver INSTANT MESSAGES to INSTANT INBOXES.

2.1 PRESENCE SERVICE

The PRESENCE SERVICE has two distinct sets of "clients" (remember, these may be combined in an implementation, but treated separately in the model). One set of clients, called PRESENTITIES, provides PRESENCE INFORMATION to be stored and distributed. The other set of clients, called WATCHERS, receives PRESENCE INFORMATION from the service.


```
          +---------------------------+
          |      PRESENCE SERVICE     |
          |                           |
          +---------------------------+
               ^                 |
               |                 |
               |                 v
      +------------+     +------------+
      | PRESENTITY |     |  WATCHER   |
      +------------+     +------------+
```

Fig. 1: Overview of Presence Service

There are two kinds of WATCHERS, called FETCHERS and SUBSCRIBERS. A FETCHER simply requests the current value of some PRESENTITY's PRESENCE INFORMATION from the PRESENCE SERVICE. In contrast, a SUBSCRIBER requests notification from the PRESENCE SERVICE of

```
         +---------------------------+
         |     PRESENCE SERVICE      |
         |           P2              |
         +---------------------------+
                                |P2
                                v
      +-------------+      +-------------+
      |     P2      |      |   P1->P2    |
      | PRESENTITY  |      | SUBSCRIBER  |
      +-------------+      +-------------+
```

Fig. 3c: NOTIFICATION (Step 3)

2.2 INSTANT MESSAGE SERVICE

The INSTANT MESSAGE SERVICE also has two distinct sets of "clients": SENDERS and INSTANT INBOXES. A SENDER provides INSTANT MESSAGES to the INSTANT MESSAGE SERVICE for delivery. Each INSTANT MESSAGE is

addressed to a particular INSTANT INBOX ADDRESS, and the INSTANT MESSAGE SERVICE attempts to deliver the message to a corresponding INSTANT INBOX.

```
         +---------------------------+
         |  INSTANT MESSAGE SERVICE  |
         |                           |
         +---------------------------+
              ^                |
              |                |
              |                v
      +-------------+      +---------------+
      |   SENDER    |      | INSTANT INBOX |
      +-------------+      +---------------+
```

Fig. 4: Overview of Instant Message Service

2.3 Protocols

A PRESENCE PROTOCOL defines the interaction between PRESENCE SERVICE, PRESENTITIES, and WATCHERS. PRESENCE INFORMATION is carried by the PRESENCE PROTOCOL.

An INSTANT MESSAGE PROTOCOL defines the interaction between INSTANT MESSAGE SERVICE, SENDERS, and INSTANT INBOXES. INSTANT MESSAGES are carried by the INSTANT MESSAGE PROTOCOL.

In terms of this model, we believe that the IMPP working group is planning to develop detailed requirements and specifications for the structure and formats of the PRESENCE PROTOCOL, PRESENCE INFORMATION, INSTANT MESSAGE PROTOCOL, and INSTANT MESSAGES.

2.4 Formats

The model defines the PRESENCE INFORMATION to consist of an arbitrary number of elements, called PRESENCE TUPLES. Each such element consists of a STATUS marker (which might convey information such as online/offline/busy/away/do not disturb), an optional COMMUNICATION ADDRESS, and optional OTHER PRESENCE MARKUP. A COMMUNICATION ADDRESS includes a COMMUNICATION MEANS and a CONTACT ADDRESS. One type of

COMMUNICATION MEANS, and the only one defined by this model, is INSTANT MESSAGE SERVICE. One type of CONTACT ADDRESS, and the only one defined by this model, is INSTANT INBOX ADDRESS. However, other possibilities exist: a COMMUNICATION MEANS might indicate some form of telephony, for example, with the corresponding CONTACT ADDRESS containing a telephone number.


```
+------------------------------------+
| PRESENCE INFORMATION               |
+------------------------------------+
 | +-------------------------------+
 =>| PRESENCE TUPLE                |
 | +-------------------------------+
 |    | +-------------------------+
 |    =>| STATUS                  |
 |    | +-------------------------+
 |    | +-------------------------+
 |    =>| COMMUNICATION ADDRESS   |
 |    | +-------------------------+
 |    |       | +-----------------+
 |    |       =>| CONTACT MEANS   |
 |    |       | +-----------------+
 |    |       | +-----------------+
 |    |       =>| CONTACT ADDRESS |
 |    |         +-----------------+
 |    | +-------------------------+
 |    =>| OTHER MARKUP            |
 |      +-------------------------+
 | +-------------------------------+
 =>| PRESENCE TUPLE                |
 | +-------------------------------+
 |    | +-------------------------+
 |    =>| STATUS                  |
 |    | +-------------------------+
 |    | +-------------------------+
 |    =>| COMMUNICATION ADDRESS   |
 |    | +-------------------------+
 |    |       | +-----------------+
 |    |       =>| CONTACT MEANS   |
 |    |       | +-----------------+
 |    |       | +-----------------+
 |    |       =>| CONTACT ADDRESS |
 |    |         +-----------------+
 |    | +-------------------------+
 |    =>| OTHER MARKUP            |
 |      +-------------------------+
 | +-------------------------------+
 =>| PRESENCE TUPLE                |
 | +-------------------------------+
 |     ...
```

Fig. 5: The structure of PRESENCE INFORMATION

STATUS is further defined by the model to have at least two states that interact with INSTANT MESSAGE delivery -- OPEN, in which INSTANT MESSAGES will be accepted, and CLOSED, in which INSTANT MESSAGES will not be accepted. OPEN and CLOSED may also be applicable to other COMMUNICATION MEANS -- OPEN mapping to some state meaning "available" or "open for business" while CLOSED means "unavailable" or "closed to business." The model allows STATUS to include other values, which may be interpretable by programs or only by persons. The model also allows STATUS to consist of single or multiple values.

2.5 Presence and its effect on Instant Messages

An INSTANT INBOX is a receptacle for INSTANT MESSAGES. Its INSTANT INBOX ADDRESS is the information that can be included in PRESENCE INFORMATION to define how an INSTANT MESSAGE should be delivered to that INSTANT INBOX. As noted above, certain values of the STATUS marker indicate whether INSTANT MESSAGES will be accepted at the INSTANT INBOX. The model does not otherwise constrain the delivery mechanism or format for instant messages. Reasonable people can disagree about whether this omission is a strength or a weakness of this model.

2.6 PRINCIPALS and their agents

This model includes other elements that are useful in characterizing how the protocol and markup work. PRINCIPALS are the people, groups, and/or software in the "real world" outside the system that use the system as a means of coordination and communication. It is entirely outside the model how the real world maps onto PRINCIPALS -- the system of model entities knows only that two distinct PRINCIPALS are distinct, and two identical PRINCIPALS are identical.

A PRINCIPAL interacts with the system via one of several user agents (INBOX USER AGENT; SENDER USER AGENT; PRESENCE USER AGENT; WATCHER USER AGENT). As usual, the different kinds of user agents are split apart in this model even though most implementations will combine at least some of them. A user agent is purely coupling between a PRINCIPAL and some core entity of the system (respectively, INSTANT INBOX; SENDER; PRESENTITY; WATCHER).


```
              +---------------------------+
              |     PRESENCE SERVICE      |
              +---------------------------+
                   ^                 |
                   | PRESENCE PROTOCOL |
                   |                 v
```

```
              +------------+        +------------+
              | PRESENTITY |        |  WATCHER   |
              +------------+        +------------+
                    ^                      ^
                    |                      |
                    |                      |
       o     +--------------+       +--------------+     o
      /|\ -->| PRESENCE UA  |       | WATCHER UA   |<-- /|\
       X     +--------------+       +--------------+     X

   (PRINCIPAL)                                        (PRINCIPAL)
```

Fig. 6: A presence system

```
              +--------------------------+
              |  INSTANT MESSAGE SERVICE |
              +--------------------------+
                  ^                    |
                IM|  INSTANT MESSAGE   |IM
                  |      PROTOCOL      v
           +------------+       +---------------+
           |   SENDER   |       | INSTANT INBOX |
           +------------+       +---------------+
                 ^                      ^
                 |                      |
                 |                      |
     o     +-------------+     +------------------+     o
    /|\ -->| SENDER UA   |     |  INBOX UA        |<-- /|\
     X     +-------------+     +------------------+     X

   (PRINCIPAL)                                       (PRINCIPAL)
```

Fig. 7: An instant messaging system

2.7 Examples

A simple example of applying the model is to describe a generic "buddy list" application. These applications typically expose the user's presence to others, and make it possible to see the presence of others. So we could describe a buddy list as the combination of a PRESENCE USER AGENT and WATCHER USER AGENT for a single PRINCIPAL, using a single PRESENTITY and a single SUBSCRIBER.

We could then extend our example to instant messaging and describe a generic "instant messenger" as essentially a buddy list with additional capabilities for sending and receiving instant messages. So an instant messenger would be the combination of a PRESENCE USER AGENT, WATCHER USER AGENT, INBOX USER AGENT, and SENDER USER AGENT for a single PRINCIPAL, using a single PRESENTITY, single SUBSCRIBER, and single INSTANT INBOX, with the PRESENTITY's PRESENCE INFORMATION including an INSTANT INBOX ADDRESS that leads to the INSTANT INBOX.

3. Model

ACCESS RULES: constraints on how a PRESENCE SERVICE makes PRESENCE INFORMATION available to WATCHERS. For each PRESENTITY's PRESENCE INFORMATION, the applicable ACCESS RULES are manipulated by the PRESENCE USER AGENT of a PRINCIPAL that controls the PRESENTITY.

Motivation: We need some way of talking about hiding presence information from people.

CLOSED: a distinguished value of the STATUS marker. In the context of INSTANT MESSAGES, this value means that the associated INSTANT INBOX ADDRESS, if any, corresponds to an INSTANT INBOX that is unable to accept an INSTANT MESSAGE. This value may have an analogous meaning for other COMMUNICATION MEANS, but any such meaning is not defined by this model. Contrast with OPEN.

COMMUNICATION ADDRESS: consists of COMMUNICATION MEANS and CONTACT ADDRESS.

COMMUNICATION MEANS: indicates a method whereby communication can take place. INSTANT MESSAGE SERVICE is one example of a COMMUNICATION MEANS.

CONTACT ADDRESS: a specific point of contact via some COMMUNICATION MEANS. When using an INSTANT MESSAGE SERVICE, the CONTACT ADDRESS is an INSTANT INBOX ADDRESS.

DELIVERY RULES: constraints on how an INSTANT MESSAGE SERVICE delivers received INSTANT MESSAGES to INSTANT INBOXES. For each INSTANT INBOX, the applicable DELIVERY RULES are manipulated by the INBOX USER AGENT of a PRINCIPAL that controls the INSTANT INBOX.

Motivation: We need a way of talking about filtering instant messages.

FETCHER: a form of WATCHER that has asked the PRESENCE SERVICE to for the PRESENCE INFORMATION of one or more PRESENTITIES, but has not asked for a SUBSCRIPTION to be created.

INBOX USER AGENT: means for a PRINCIPAL to manipulate zero or more INSTANT INBOXES controlled by that PRINCIPAL.

Motivation: This is intended to isolate the core functionality of an INSTANT INBOX from how it might appear to be manipulated by a product. This manipulation includes fetching messages, deleting messages, and setting DELIVERY RULES. We deliberately take no position on whether the INBOX USER AGENT, INSTANT INBOX, and INSTANT MESSAGE SERVICE are colocated or distributed across machines.

INSTANT INBOX: receptacle for INSTANT MESSAGES intended to be read by the INSTANT INBOX's PRINCIPAL.

INSTANT INBOX ADDRESS: indicates whether and how the PRESENTITY's

PRINCIPAL can receive an INSTANT MESSAGE in an INSTANT INBOX. The STATUS and INSTANT INBOX ADDRESS information are sufficient to determine whether the PRINCIPAL appears ready to accept the INSTANT MESSAGE.

Motivation: The definition is pretty loose about exactly how any of this works, even leaving open the possibility of reusing parts of the email infrastructure for instant messaging.

INSTANT MESSAGE: an identifiable unit of data, of small size, to be sent to an INSTANT INBOX.

Motivation: We do not define "small" but we seek in this definition to avoid the possibility of transporting an arbitrary-length stream labelled as an "instant message."

INSTANT MESSAGE PROTOCOL: The messages that can be exchanged between a SENDER USER AGENT and an INSTANT MESSAGE SERVICE, or between an INSTANT MESSAGE SERVICE and an INSTANT INBOX.

INSTANT MESSAGE SERVICE: accepts and delivers INSTANT MESSAGES.

-- May require authentication of SENDER USER AGENTS and/or INSTANT INBOXES.

-- May have different authentication requirements for different INSTANT INBOXES, and may also have different authentication requirements for different INSTANT INBOXES controlled by a single PRINCIPAL.

-- May have an internal structure involving multiple SERVERS and/or PROXIES. There may be complex patterns of redirection and/or proxying while retaining logical connectivity to a single INSTANT MESSAGE SERVICE. Note that an INSTANT MESSAGE SERVICE does not require having a distinct SERVER -- the service may be implemented as direct communication between SENDER and INSTANT INBOX.

-- May have an internal structure involving other INSTANT MESSAGE SERVICES, which may be independently accessible in their own right as well as being reachable through the initial INSTANT MESSAGE SERVICE.

NOTIFICATION: a message sent from the PRESENCE SERVICE to a SUBSCRIBER when there is a change in the PRESENCE INFORMATION of some PRESENTITY of interest, as recorded in one or more SUBSCRIPTIONS.

Motivation: We deliberately take no position on what part of the changed information is included in a NOTIFICATION.

OPEN: a distinguished value of the STATUS marker. In the context of INSTANT MESSAGES, this value means that the associated INSTANT INBOX ADDRESS, if any, corresponds to an INSTANT INBOX that is ready to accept an INSTANT MESSAGE. This value may have an

analogous meaning for other COMMUNICATION MEANS, but any such meaning is not defined by this model. Contrast with CLOSED.

OTHER PRESENCE MARKUP: any additional information included in the PRESENCE INFORMATION of a PRESENTITY. The model does not define this further.

POLLER: a FETCHER that requests PRESENCE INFORMATION on a regular basis.

PRESENCE INFORMATION: consists of one or more PRESENCE TUPLES.

PRESENCE PROTOCOL: The messages that can be exchanged between a PRESENTITY and a PRESENCE SERVICE, or a WATCHER and a PRESENCE SERVICE.

PRESENCE SERVICE: accepts, stores, and distributes PRESENCE INFORMATION.

-- May require authentication of PRESENTITIES, and/or WATCHERS.

-- May have different authentication requirements for different PRESENTITIES.

-- May have different authentication requirements for different WATCHERS, and may also have different authentication requirements for different PRESENTITIES being watched by a single WATCHER.

-- May have an internal structure involving multiple SERVERS and/or PROXIES. There may be complex patterns of redirection and/or proxying while retaining logical connectivity to a single PRESENCE SERVICE. Note that a PRESENCE SERVICE does not require having a distinct SERVER -- the service may be implemented as direct communication among PRESENTITY and WATCHERS.

-- May have an internal structure involving other PRESENCE SERVICES, which may be independently accessible in their own right as well as being reachable through the initial PRESENCE SERVICE.

PRESENCE TUPLE: consists of a STATUS, an optional COMMUNICATION ADDRESS, and optional OTHER PRESENCE MARKUP.

PRESENCE USER AGENT: means for a PRINCIPAL to manipulate zero or more PRESENTITIES.

Motivation: This is essentially a "model/view" distinction: the PRESENTITY is the model of the presence being exposed, and is independent of its manifestation in any user interface. In addition, we deliberately take no position on how the PRESENCE USER AGENT, PRESENTITY, and PRESENCE SERVICE are colocated or distributed across machines.

PRESENTITY (presence entity): provides PRESENCE INFORMATION to a PRESENCE SERVICE.

Motivation: We don't like to coin new words, but "presentity" seemed worthwhile so as to have an unambiguous term for the entity of interest to a presence service. Note that the presentity is not (usually) located in the presence service: the presence service only has a recent version of the presentity's presence information. The presentity initiates changes in the presence information to be distributed by the presence service.

PRINCIPAL: human, program, or collection of humans and/or programs that chooses to appear to the PRESENCE SERVICE as a single actor, distinct from all other PRINCIPALS.

Motivation: We need a clear notion of the actors outside the system. "Principal" seems as good a term as any.

PROXY: a SERVER that communicates PRESENCE INFORMATION, INSTANT MESSAGES, SUBSCRIPTIONS and/or NOTIFICATIONS to another SERVER. Sometimes a PROXY acts on behalf of a PRESENTITY, WATCHER, or INSTANT INBOX.

SENDER: source of INSTANT MESSAGES to be delivered by the INSTANT MESSAGE SERVICE.

SENDER USER AGENT: means for a PRINCIPAL to manipulate zero or more SENDERS.

SERVER: an indivisible unit of a PRESENCE SERVICE or INSTANT MESSAGE SERVICE.

SPAM: unwanted INSTANT MESSAGES.

SPOOFING: a PRINCIPAL improperly imitating another PRINCIPAL.

STALKING: using PRESENCE INFORMATION to infer the whereabouts of a PRINCIPAL, especially for malicious or illegal purposes.

STATUS: a distinguished part of the PRESENCE INFORMATION of a PRESENTITY. STATUS has at least the mutually-exclusive values OPEN and CLOSED, which have meaning for the acceptance of INSTANT MESSAGES, and may have meaning for other COMMUNICATION MEANS. There may be other values of STATUS that do not imply anything about INSTANT MESSAGE acceptance. These other values of STATUS may be combined with OPEN and CLOSED or they may be mutually-exclusive with those values.

Some implementations may combine STATUS with other entities. For example, an implementation might make an INSTANT INBOX ADDRESS visible only when the INSTANT INBOX can accept an INSTANT MESSAGE. Then, the existence of an INSTANT INBOX ADDRESS implies OPEN, while its absence implies CLOSED.

SUBSCRIBER: a form of WATCHER that has asked the PRESENCE SERVICE to notify it immediately of changes in the PRESENCE INFORMATION of one or more PRESENTITIES.

SUBSCRIPTION: the information kept by the PRESENCE SERVICE about a SUBSCRIBER's request to be notified of changes in the PRESENCE INFORMATION of one or more PRESENTITIES.

VISIBILITY RULES: constraints on how a PRESENCE SERVICE makes WATCHER INFORMATION available to WATCHERS. For each WATCHER's WATCHER INFORMATION, the applicable VISIBILITY RULES are manipulated by the WATCHER USER AGENT of a PRINCIPAL that controls the WATCHER.

Motivation: We need a way of talking about hiding watcher information from people.

WATCHER: requests PRESENCE INFORMATION about a PRESENTITY, or WATCHER INFORMATION about a WATCHER, from the PRESENCE SERVICE. Special types of WATCHER are FETCHER, POLLER, and SUBSCRIBER.

WATCHER INFORMATION: information about WATCHERS that have received PRESENCE INFORMATION about a particular PRESENTITY within a particular recent span of time. WATCHER INFORMATION is maintained by the PRESENCE SERVICE, which may choose to present it in the same form as PRESENCE INFORMATION; that is, the service may choose to make WATCHERS look like a special form of PRESENTITY.

Motivation: If a PRESENTITY wants to know who knows about it, it is not enough to examine only information about SUBSCRIPTIONS. A WATCHER might repeatedly fetch information without ever subscribing. Alternately, a WATCHER might repeatedly subscribe, then cancel the SUBSCRIPTION. Such WATCHERS should be visible to the PRESENTITY if the PRESENCE SERVICE offers WATCHER INFORMATION, but will not be appropriately visible if the WATCHER INFORMATION includes only SUBSCRIPTIONS.

WATCHER USER AGENT: means for a PRINCIPAL to manipulate zero or more WATCHERS controlled by that PRINCIPAL.

Motivation: As with PRESENCE USER AGENT and PRESENTITY, the distinction here is intended to isolate the core functionality of a WATCHER from how it might appear to be manipulated by a product. As pre

"MP3 Recorder Download - MP3 Recorder - Record Audio Stream to MP3 or WAV," 2002 ttp://www.mp3-recorder.net

STRATEGIC COMPUTER TECHNOLOGY

DATA CONNECTION

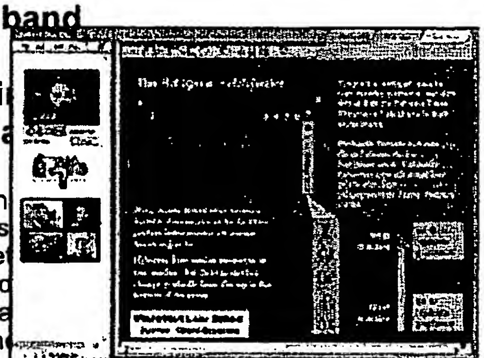
Company
Products
Careers
Contact Us
Home
News
Search

MeetingServer

Broadband for Learning Case Study

Data Connection's MeetingServer has been chosen as a key component of the Broadband for Learning project, providing conferencing solutions for a variety of education applications. Initially being rolled out in 120 locations across North London, the Broadband for Learning project connects PC-based conferencing systems in schools, colleges and learning centres, as well as allowing students to access the system from home. MeetingServer provides web conferencing capabilities, so that users can share applications, presentations and a whiteboard.

Broadband for Learni applica



Bi-lingual science lesson - Broadband for Learning joins classrooms in different schools

- Sh les be mo tha on sch - even sharing language teaching sessions from other countries
- Teacher-pupil meetings on-line - for example to talk about assignments
- Sharing materials - and experience - among teachers and trainers through on-line document sharing
- Trainer/trainee progress reviews
- On-line career guidance

Broadband for Learning solution

The Broadband for Learning project was co-ordinated by Apperception, who assessed a number of competing solutions, and chose a system integrated by VAvox, comprising a SIP-based audio and video conferencing system using a hardware MCU, alongside MeetingServer's web conferencing facilities.

Messaging
MailNGen
Voicemail
Email
Unified Messaging

Conferencing
MeetingServer
Architecture and integration
Case Study

Directory
Overview
Directories Explained
DC-Directory
DC-Metalink

Technology For OEMs
OEM Solutions

Resources
Press Releases
Support
Quality
Customers
Company

FROST & SULLIVAN

Data Connection wins conferencing and collaboration award

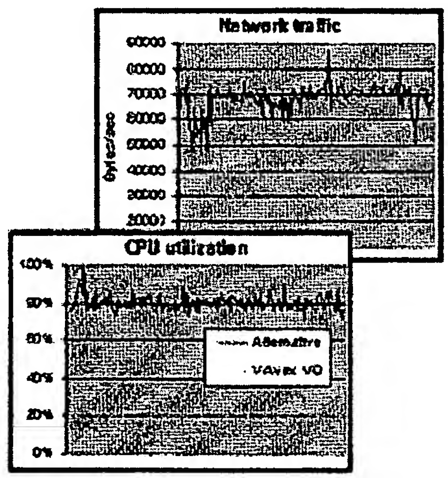
VAvox combine these tools behind an integrated interface known as VAvox VQ.

MeetingServer was chosen for this solution because it provides an intuitive and robust user experience, it is easy to integrate, and it out-performs the alternatives.

User experience

For many of Broadband for Learning's typical users, using a computer is a relatively unusual activity, so the conferencing tools have to be easy-to-use. MeetingServer's intuitive interface fits the bill.

The system has to be robust. Users will abandon even the most powerful features if they are prone to failure. VAvox and Apperception carried out extensive testing to ensure that MeetingServer met their rigorous reliability standards.



The VAvox VQ system, incorporating MeetingServer, uses significantly less bandwidth and CPU than other conferencing solutions

Source: Apperception competitive analysis, September 2003

Ease of integration

VAvox engineers integrated MeetingServer in less than two weeks. MeetingServer conferences can be accessed through single-click URLs, and it was simple to include these links within the VAvox VQ interface.

The URLs include user information so that participants can be authenticated as they access a conference - crucial in a guidance situation discussing confidential information.

Performance

Many education institutions have relatively low-powered computing and networking equipment, and pupils or trainees joining a Broadband for Learning session may not have the latest PC technology at home. To make the system open to the widest user base, the conferencing technology has to be efficient in network bandwidth and CPU power required.

Apperception evaluated the VAvox VQ system, incorporating MeetingServer, alongside alternative, commercially available conferencing packages, and proved it to be much more efficient in both measures.

For more information about Data Connection's conferencing solutions, please contact meetingserver@dataconnection.com.

MailNGen

Next Generation Messaging for Service Providers

DATA CONNECTION

MailNGen is a flexible, modular multimedia messaging solution, allowing Service Providers to deploy a range of voicemail, email, webmail and fax message services through a single mailbox universally accessible from the phone or the desktop. By enabling mailbox access using VoIP and HTTP, in a scalable IP-distributed architecture, MailNGen truly offers messaging for next generation networks.

Applications

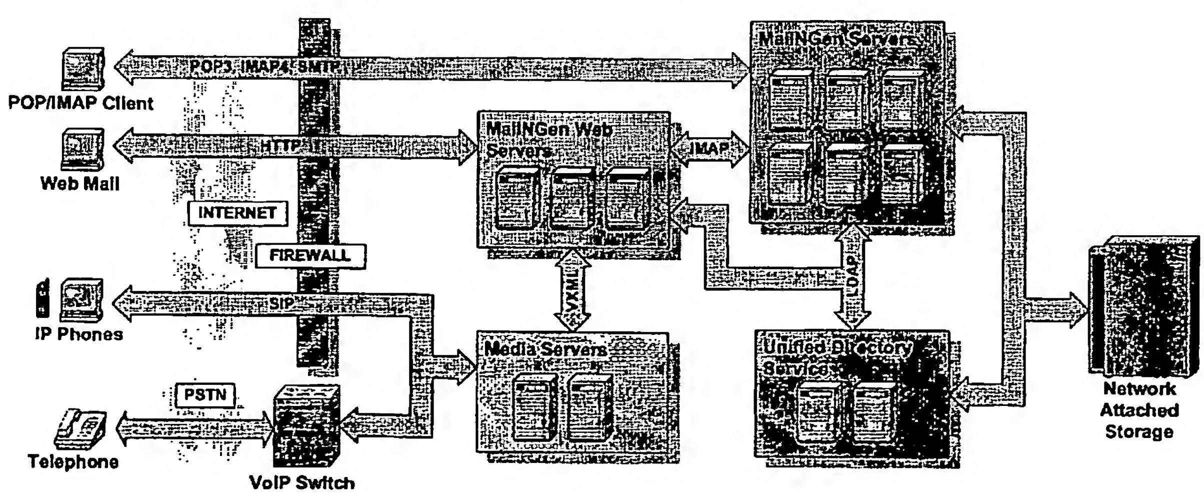
Suitable for small deployments as well as high-availability multi-million user environments, MailNGen can be used in anything from a basic voicemail or email system through to sophisticated unified messaging with universal access to all media types.

- Internet email using standard third-party clients, as well as a fully rebrandable webmail interface.
- Voicemail accessible from SIP as well as POTS phones, using Voice XML standards.
- Full unified messaging with all media type messages stored in a single mailbox. Listen to emails by phone, play voicemails over the web, forward faxes as emails – all through rebrandable phone and desktop interfaces

Benefits for Service Providers

- Rich range of features, with an easy upgrade path from basic email or voicemail to full unified messaging.
- Proven carrier-class scalability to millions of mailboxes on a single, centrally administered, fault-tolerant system.
- Fully customizable web and telephony UIs allowing rebranding, including virtual SP support.
- Reduced hardware costs – MailNGen runs on standard off-the-shelf O/S and hardware equipment.
- Complete range of user functions, with web and telephony self-care to reduce operating costs.

MailNGen in a unified messaging deployment



Security

MailNGen's security features include

- protection against DoS attacks
- mailbox shutout after failed logons
- protection against open relay (anti-spam)
- restrict mailbox access by IP address.

Client access

- Standard email clients (SMTP, POP, IMAP).
- Intuitive and fully re-brandable multi-foldered webmail client.
- VXML access, using off-the-shelf browsers, gives full-function voice access. TUI is fully customizable and can be matched to legacy voicemail systems.

Management

- Web, GUI and CLI tools are provided for directory-based administration (LDAP).
- Bulk provisioning tools simplify deployment.
- Rich statistics gathering and reporting.
- Multiple independent message stores aid easy backup administration.

Supported platforms

MailNGen software is independent of the OS or hardware platform. Packaged versions are available for Solaris, Red Hat Linux and HP-UX.

Performance, reliability and scalability

MailNGen's distributed data store enables high-performance and high-availability.

- Mailboxes not tied to individual servers – all mailboxes accessible even on server failure.
- Bottleneck-free architecture provides linear scalability, with auto-discovery of newly installed servers.
- System components can be deployed in any ratio – for example to cope with varying proportions of web and IMAP users.

Specialist support and services

- Customer support is resourced from Data Connection's original development teams.
- Unlimited support is available by phone and email with guaranteed response times.
- Training and integration services (such as integration with billing system) can be provided.

About Data Connection

Data Connection Limited (DCL) is the leading independent developer and supplier of Messaging, Directory, Conferencing, SIP, MGCP/Megaco, MPLS, IP Routing, ATM, SS7, and SNA portable software products.

Customers for Data Connection's messaging products include SBC, Verizon, COLT Telecom, Cisco, Microsoft, Lotus, Comverse Networks, Lockheed Martin, and Unisys.

Data Connection is headquartered in London UK, with US offices in Reston, VA and Alameda, CA, and has around 275 employees of whom 210 are software engineers. It is independently owned and entirely self-funding.

Data Connection's profits have exceeded 20% of revenue each year since it was founded in 1981. Last year sales exceeded $39 million, of which 90% were outside the UK, mostly in the US.

Contact information

Email: mailngen@dataconnection.com

North America
Phone: +1 703 715 4914

Data Connection Corporation
12007 Sunrise Valley Drive
Suite 250
Reston
Virginia 20191

Worldwide
Phone: +44 20 8366 1177

Data Connection Ltd.
100 Church Street
Enfield EN2 6BQ
UK

www.dataconnection.com

www.mailngen.com

DATA CONNECTION

STRATEGIC COMPUTER TECHNOLOGY

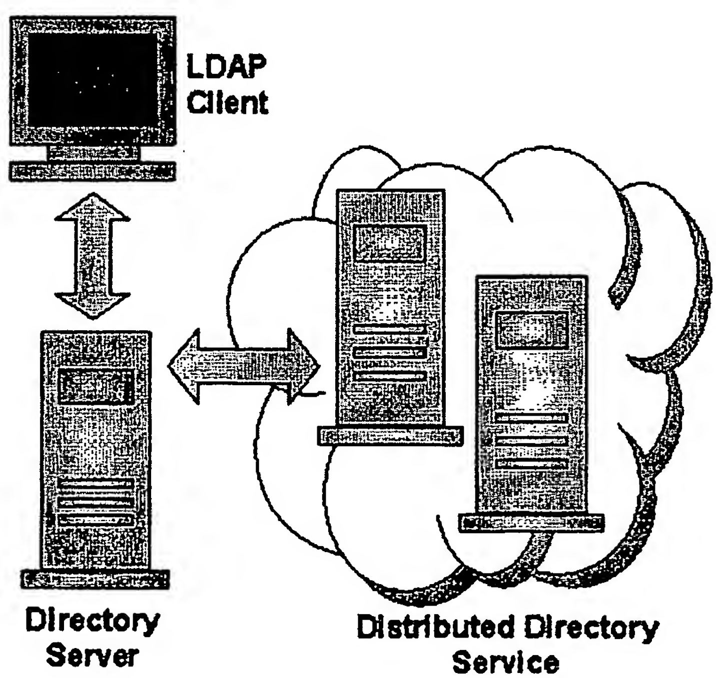
Company
Products
Careers
Contact Us
Home
News
Search

Directories Explained

Directories are a special type of database. They are designed to hold information about the people, resources and policies that are of interest to network applications, services and devices. There are international standards for directories, notably LDAP, the most common client access protocol, and X.500. Directories have grown rapidly in importance because of the dramatic and continuing growth in the number of deployed network solutions.

The information in a directory is held as a series of entries organized in a family tree-like hierarchy, and is most usually accessed by directory clients using LDAP.

Directory data can be held in a single directory server, perhaps integrated as part of an application, service or device. That directory server can also cooperate with other directory servers, typically using the X.500 protocols, to form part of a distributed directory service.



Directories and Relational Databases

There are some important differences between directories and relational databases.

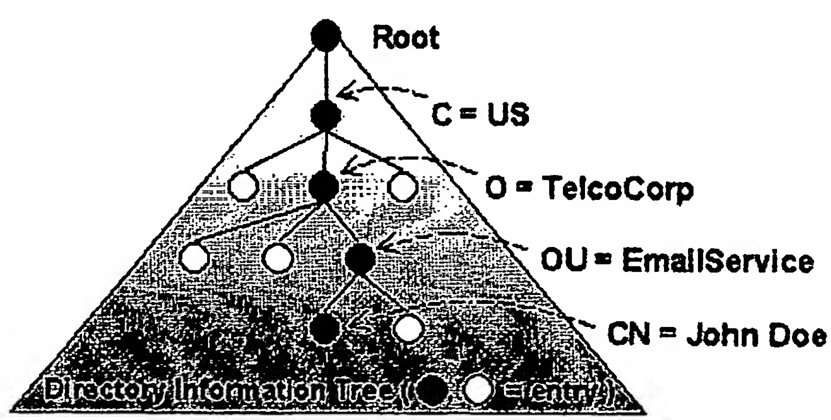
Mess
MailNG
Voicem
Email
Unified
Conf
Meetin
Archite
Case S
Direc
Overvi
Directo
DC-Dir
DC-Me
Tech
OEM
OEM S
Reso
Press I
Suppo
Quality
Custon
Compa

- Directories make the design assumption that the data they hold will be read much more often than it is changed (just as a paper telephone directory is used much more often than it is reprinted). As a result, they incorporate indexing technology that is highly optimized for read and search performance.
- In comparison to relational databases, directories offer fine-grained flexibility over where particular data is held around a network, and who has rights to administer it. Distributed operation is a design requirement for directories.
- The protocols used to access directories, usually LDAP, provide deliberately limited facilities. For example, there is currently no standard for "transactions" to maintain integrity between directory entries, nor operations to manage large unstructured binary data. Directories are not intended as a general-purpose replacement for RDBMS or file systems.

Inevitably, these differences are blurred in reality, usually for reasons of legacy migration - with some directory-focused technologies being used to provide more general database features, and with relational databases used to store hierarchical data. Where a product requires both directory and relational database views of its data, the most powerful option is to have both and synchronize between them using a meta-directory (see Meta-Directories Explained).

Directory Information Tree and Directory Schema

The **directory information tree** is the hierarchical "family tree" of entries held in the directory (possibly distributed across many different directory servers). Each entry in the tree typically corresponds to a particular resource such as a user or group. Each entry is the "child" of the entry above it in the tree, stretching back to the master "root" entry. The following diagram shows an example where an organization called TelcoCorp has organized the directory information tree by service type (EmailService) and then by subscriber (John Doe).



The **directory schema** is the collection or rules about what can be held in the directory and the structure of the directory information tree. For example,

the schema can define

- the information that can or must be held in each type of directory entry - the schema for directory tree shown in the diagram might specify that user entries have to include an email address
- which entries can be placed as "children" of which other entries - the schema for the tree shown might specify that users have to appear "under" an organizational unit

The LDAP and X.500 standards define a number of schema rules, which directory servers can choose to support and police. The broader the checking, the more directory clients can depend on the information in the directory to be well formatted.

There are a number of standard directory schemas that have been defined to simplify the interoperability of directory clients and servers, such as the **inetOrgPerson** schema for users.

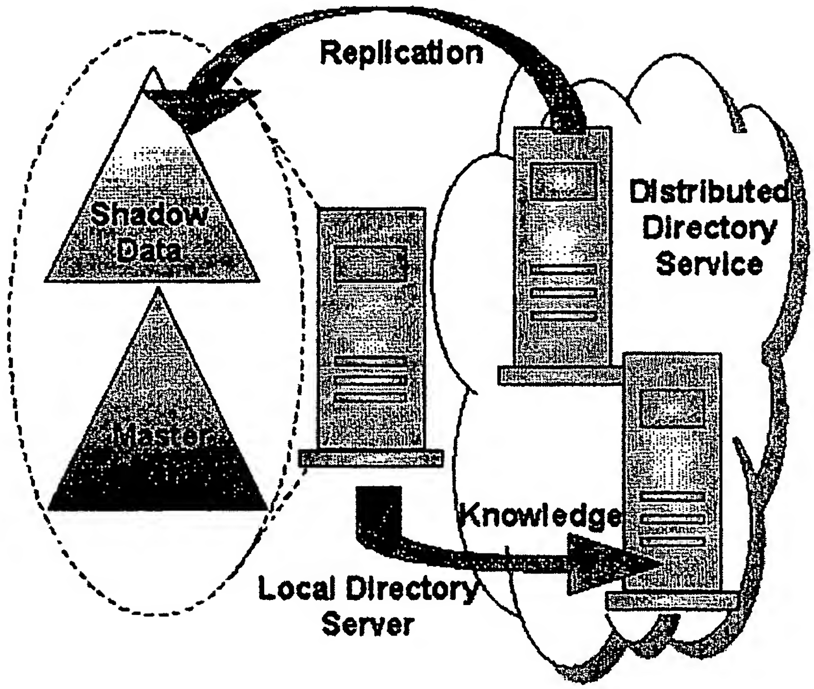
Distributed Directory Services and Access Control

Directory clients can search, read and update the directory using LDAP to access a directory server. The directory server that is accessed might contain all the data to satisfy the request itself, or it might need to co-operate with other servers as part of a distributed directory service.

The hierarchical tree of directory entries allows great flexibility in the distribution of directory data between servers.

- The master copy of particular parts of the directory tree can be assigned to particular directory servers. As an example, each server might be configured to master data for resources that are geographically or organizationally "local".
- In addition to its master data, each server can hold a shadow copy of all or part of the data mastered on other servers.
- Finally, there may be data in the directory for which a server holds neither a master nor a shadow copy. In this case, it will maintain "knowledge" of where to find the data in its peer servers.

For all of this operation, the X.500 protocols are typically used to support the interactions between distributed directory servers (see Meta-Directories Explained for a discussion of multi-master configurations).



Distributed administration of directory data is supported by the directory's **access control**. This data specifies which users are allowed to view, read and change particular parts of the tree. This allows for delegated administration of particular parts of the directory (for example, a local administrator whose rights are limited to the data for his or her part of the network).

To ensure the integrity of a distributed directory, it is very important that access control is distributed and synchronized along with the directory data it polices.

MetaDirectories Explained

Meta-directories are applications that often work alongside directories. They provide facilities to manage information about people, resources and policies that is spread, and possibly duplicated, across more than one directory or database. Meta-directories have grown rapidly in importance because it is seldom practical for all such information to be held and mastered in a single data store.

Specifically, there are two common issues with implementing the pure directory model described above.

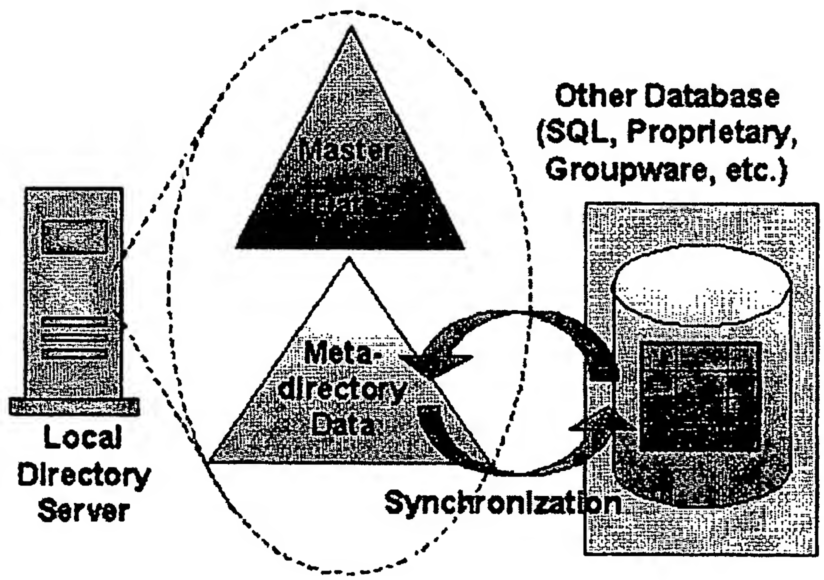
- First, relevant data for an application or service may be already held and "owned" in multiple and varied data stores, including enterprise directories, groupware systems, relational databases, and so on. A directory service must co-exist with, rather than replace, these existing data stores.
- Second, the shadowing of readable copies of directory data and the distribution of master data across multiple servers is not enough to

meet today's most demanding availability requirements. In the pure directory model, the master copy for each entry remains a "single point of failure".

Meta-directories address these issues, whether as standalone products or as integrated components of a directory server.

Synchronization between different data stores

The first major use of meta-directories is to tie together data held in disparate data stores.



The illustration above shows a simple example of meta-directory synchronization where rows in a relational database table are kept in step with entries in a directory server. The data can be read using either SQL access to the relational database or LDAP access to the directory. If a change is made in the database, then the equivalent change is automatically made to the directory, and vice versa.

There are many examples where meta-directory synchronization is able to address a network solution vendor requirement. Two common examples are as follows.

- An existing product developed on top of a relational database may want to take advantage of user and group data held in already-deployed enterprise directories. A meta-directory is able to populate the relational database with that data and then keep it in step, without requiring changes to the existing product. This removes the need for manual configuration and ongoing administration of the product data.
- A directory-enabled network device may be administered using a hierarchical distributed directory, but require a local highly-optimized data store for its operational configuration data. A meta-directory is

able to populate the local data store with data and refresh it with configuration changes as they occur.

To meet these requirements, meta-directories need to be readily extensible to support different data stores and to cope with different types of mapping between the objects, records and entries that each store holds.

They also need to have all the flexibility of standards-based distributed directory scheduling - including fine-grained control on when synchronization occurs and which attributes and entries are kept in step between systems.

Finally, the goal for meta-directories is to minimize the impact on the synchronized systems (which may provide only limited access rights to the meta-directory), and to achieve all the above through configuration rather than extensive engineering consultancy and customized development services.

Multi-mastering

The second major use of meta-directories is to support multi-mastering of directory data.

In the standard directory model, there is a single master copy of each directory entry. While shadow copies can be readily configured to provide high availability for read access to the directory (and for many requirements this is sufficient), the model still presents a single point of failure for writes and updates.

To address this it is necessary to move to a multi-master architecture where there are two or more master copies of each directory entry. In practical terms this is achieved using meta-directory synchronization.

- Meta-directory synchronization is configured between the two peer directory servers each holding an independent "master" copy of the same directory entries.
- Changes to each of the directory servers are mirrored to the other by the meta-directory, keeping the two servers in step.
- As with a pure distributed directory, it is vital that access control information is held in step on the two servers to ensure the integrity of the overall system.
- It is also important to have a policy for avoiding or resolving clashing updates (when both copies of a master are updated at the same time). This issue does not apply to the pure directory model.

With a meta-directory that is closely integrated with its associated directory server, this approach to multi-mastering allows simple configuration, because all synchronization is mapping like-for-like, and efficient operation.

Other uses of meta-directories

Finally, the synchronization function of meta-directories is extremely powerful and can be deployed to meet other requirements in addition to the data synchronization and multi-mastering noted above.

- The translation features of the meta-directory make it possible to maintain different "views" of the same directory data in a single directory server. This is important if different services using the directory expect data in different formats. For example, one service might want user entries arranged hierarchically by organizational role, the other might want users represented by a different type of entry grouped by geographical location. The meta-directory can provide both views simultaneously and ensure they are kept in step.
- The entry and attribute filtering features of the meta-directory allow it to synchronize a subset of the data in a directory to a "border directory server", with more lenient access control. The most common requirement for this is to allow publication of a restricted subset of the data in a directory for unsecured access from the Internet.
- Meta-directories can also provide "triggering" mechanisms where changes in a data store can trigger user-defined actions in addition or instead of any data synchronization. For example, when a new configuration is added to a network device, the meta-directory can initiate associated setup actions.

In addition, the synchronization and triggering functions of a meta-directory can be used to satisfy many other requirements where data needs to be accessed or available in multiple formats or multiple data stores.

email: info@dataconnection.com

Directory Systems

Directories and Meta-Directories

Directories are a special type of database. They are designed to hold information about the people, resources and policies that are of interest to network applications, services and devices. There are international standards for directories, notably LDAP, the most common client access protocol, and X.500. Directories have grown rapidly in importance because of the dramatic and continuing growth in the number of deployed network solutions.

Meta-directories are applications that often work alongside directories. They provide facilities to manage information about people, resources and policies that is spread, and possibly duplicated, across more than one directory or database. Meta-directories have grown rapidly in importance because it is seldom practical for all such information to be held and mastered in a single data store.

For more on directories and meta-directories and how they are used, see Directories and Meta-Directories Explained.

DC-Directory and DC-MetaLink

DC-Directory is a high-function directory, supporting the best elements of the LDAP and X.500 standards. Furthermore, it incorporates a tightly integrated meta-directory providing many synchronization options with other data stores. DCL licenses DC-Directory to network solution vendors who need their application, service or device to play a strategic part in the directory-enabled world. DCL works closely with the vendor to integrate DC-Directory and ensure it meets the vendor's requirements.

DC-MetaLink is a packaged version of the meta-directory features of DC-Directory. DCL licenses it to

Messaging
MailNGen
Voicemail
Email
Unified Messaging

Conferencing
MeetingServer
Architecture and integration
Case Study

Directory
Overview
Directories Explained
DC-Directory
DC-Metalink

Technology For OEMs
OEM Solutions

Resources
Press Releases
Support
Quality
Customers
Company

network solution vendors who have a specific requirement for meta-directory synchronization. For example, the vendor may want to pull in data from enterprise directories or groupware systems. Just as with DC-Directory, DCL works closely with the vendor to ensure successful integration.

As well as licensing DC-Directory to network solution vendors, DCL also markets and deploys it for service providers as the comprehensive directory infrastructure for their application services. Those application services typically include DCL's own unified messaging, white pages, conferencing, and authorization solutions.

For more detailed technical specifications see DC-Directory and DC-MetaLink, or download the Product Overview (PDF format, 273 KB).

Further information

For further information or sales enquiries about DC-Directory and DC-MetaLink, please contact directories@dataconnection.com or call Nigel Hubbard on +44 20 8366 1177.

Data Connection Home Page

STRATEGIC COMPUTER TECHNOLOGY

CONNECTION

Company
Products
Recruitment
Contact Us
Home
News

DC-IMS\Voice Unified Messaging Gateway

Messaging

DC-UniStore

SurroundSuite for Service Providers

- DC-SurroundStore
- DC-SyncroMail
- DC-IMS\Voice
- DC-Directory

SurroundSuite for Enterprises

Core Messaging Solutions

Customers

Why DCL?

DC-IMS\Voice provides a backbone "gateway" between the worlds of store-and-forward e-mail, legacy voice-mail systems, and newer wireless and wireline voice messaging systems.

- Voice Messaging Systems (VMSs) support a variety of different protocols which limits interoperability. These VMS products need to be interconnected via gateways to bring voicemail user communities together.
- Voice Mail networks need to be able to link to email networks which are now beginning to support desktop applications which can send and receive voice messages.
- Both Voice Mail and email networks need to be able to make use of the new messaging capabilities provided by today's cellular handsets.

DC-IMS\Voice is designed to address these needs, by providing a reliable, scalable gateway which links together today's voicemail systems with the Internet and with wireless devices.

Product Features

Based on the proven capabilities of DC-IMS (Integrated Messaging Server) product, DC-IMS\Voice functionality goes far beyond the level of open standards-based protocol support. It is a powerful product, not simply because of the interoperability it affords, but also because of the rich, high-performance messaging service it provides, including

- key Internet messaging standards for VPIM, including advanced ESMTP and MIME features
- supporting the key 1992, 1988 and legacy 1984 X.400 Standards, including AMIS-D
- providing a seamless, integrated gateway between VPIM and AMIS-D

- supporting gatewaying from e-mail to Short Message Service (SMS) Centres
- integration with X.500 and LDAP directory services
- support for system monitoring by SNMP agents
- operating on Windows NT and UNIX platforms
- scalable to 100's of concurrent connections with throughput of 100,000s of messages per hour
- providing comprehensive system management features.

For further information, download the DC-IMS\Voice Product Overview (self-extracting PKZIPped Word 6 format or UNIX compressed postscript format), or contact messaging@dataconnection.com.

Home
email: info@dataconnection.com

STRATEGIC SOFTWARE TECHNOLOGY

Company
Products
Recruitment
Contact Us
Home
News

DC-SurroundSuite for Service Providers

The SurroundSuite™ product family offers Unified Messaging solutions which combine Data Connection's best-of-breed datacomms and telecomms software products with leading industry messaging clients and servers.

A key requirement for Service Providers is the ability to provide new value-add services to differentiate their product offerings, while minimising the cost of administration and management of these services. The SurroundSuite™ product family achieves this by providing a comprehensive range of products that can be used selectively or in combination, to enhance service offerings without demanding replacement of existing legacy systems.

Messaging
DC-UniStore
SurroundSuite for Service Providers
- DC-SurroundStore
- DC-SyncroMail
- DC-IMS\Voice
- DC-Directory

SurroundSuite for Enterprises
Core Messaging Solutions
Customers
Why DCL?

DC-SurroundStore

DC-SurroundStore can integrate with a Service Provider's existing Internet E-Mail service (or multiple independent services) to unify voice-mail, e-mail and fax communications in order to deliver a comprehensive single-mailbox solution.

Message browsing, send/reply, forwarding, and message management are available from PCs and/or touch-tone phones, regardless of message origin and format. Features include text-to-speech conversion, single-interface administration, LDAP/X.500 directory support, and fax-mail services.

The Service Provider version of DC-SurroundStore provides far more than "just" telephone access to mail. For example:

- The telephony server component within DC-SurroundStore enables telephone users to browse through available directory services, obtain details of entries, auto-connect their phone calls, send e-mails, voice-mails or faxes, and even browse their favourite public web-sites (e.g. for weather reports, share prices) or hosted Intranets (for corporate

data).

- ☐ DC-SurroundStore can be connected to CPE messaging systems, thus allowing the Service Provider to increase the range of outsourced services that can be offered to corporations by providing telephony value-add to in-house groupware systems.
- ☐ An integrated H.323 server enables direct voice and data communications over the IP infrastructure, thus establishing an integrated Voice over IP service for messaging access.
- ☐ Using the unique web-based IVR system within DC-SurroundStore, the Service Provider can create a tailored range of phone-accessible applications for their customer base that can provide new revenue generation either by service subscription or phone tolls.

For more information on DC-SurroundStore, contact messaging@dataconnection.com.

DC-SyncroMail

DC-SyncroMail is designed to address a key issue in Unified Messaging - how do you cope with environments where service users each have multiple mailboxes? For example:

- ☐ The Service Provider may not yet be in a position to offer a combined e-mail and voice-mail service in one mailbox, and thus needs an interim solution that provides some level of user-controlled management of the multiple mailboxes.
- ☐ A user may wish to have the data from his or her residential mailbox (or mailboxes) integrated and accessible via the outsourced corporate service.
- ☐ The Service Provider needs to be able to offer migration services to users of competitive services, in order to win their business.

In all these situations, the ease-of-use of a single unified mailbox is simply not available. This is where DC-SyncroMail comes in.

DC-SyncroMail acts as an Intelligent Agent server for a user community, where each user can register personalized rules for how to manage a collection of his or her own mailboxes. Features include:

- ☐ selective forwarding of new mail to other mailboxes (including content conversion as appropriate)
- ☐

- automatic update of message status for duplicate mails in different mailboxes (read-status, deletions, etc)
- priority notifications (e-mail, voice-mail, cellular, pager)
- synchronised folder management
- hierarchical defaults and delegated administration
- full auditing and billing controls.

In summary, DC-SyncroMail has no place in the idealistic world of single-instance universal mailbox and global directories, but is designed to address major issues to do with the reality of providing Unified Messaging services in a non-unified world.

DC-SyncroMail is available later in 1999. For more information, contact messaging@dataconnection.com.

DC-IMS\Voice

DC-IMS\Voice is a standalone Universal Messaging backbone gateway which employs industry-standard voice and data protocols such as VPIM, AMIS and SMS to connect existing VoiceMail Systems with the Internet, desktop messaging systems, and wireless networks.

For more information on DC-IMS\Voice, click here .

DC-Directory

DC-Directory is a complete directory solution which combines the best elements of X.500 and Internet standards (LDAP, HTTP) with comprehensive management and administration applications to provide an open, scalable directory service for service providers and large enterprises.

In the context of Unified Messaging, DC Directory provides a complete directory infrastructure for provisioning and administration, including delegated authority, meta-directory connectors to legacy databases, and support for e-mail and voice-mail directory services.

However, the applicability of DC Directory goes far beyond Unified Messaging. DC Directory

can provide a complete electronic directory infrastructure for the Service Provider's full range of services, including conferencing, E-commerce and Public Key security services.

For more information on DC-Directory, click here .

Core Messaging Solutions

For Service Providers who are seeking a major upgrade to their core messaging infrastructure, Data Connection can also deliver first-class messaging mailbox and store-and-forward servers, which can be deployed individually to upgrade core services, or in conjunction with the SurroundSuite™ products to provide a comprehensive solution.

For more information on Data Connection's Core Messaging products, click here .

Home
email: info@dataconnection.com

Messaging Software Products and Services

Data Connection supplies a comprehensive range of messaging software products which have already been adopted in a wide range of services and solutions in the messaging industry.

- Product vendors employ our software within their messaging server solutions to provide high-function industry-standard message protocol support.
- Service Providers and large end-user organizations use our software to build high-end message backbone infrastructures.
- Systems Integrators use our technology and engineering expertise to help them create unique messaging solutions to address complex client requirements.

Using our unique portable software product architecture, Data Connection's messaging products are available on a wide range of platforms, including Solaris, HP-UX, AIX, and Windows NT ®.

Unified Messaging Solutions

Data Connection has a unique breadth of software expertise that spans both the data communications and telecommunications marketplaces. This enables us to provide a comprehensive range of products which provide Unified Messaging solutions.

DC-UniStore

DC-UniStore is a complete Internet-based Unified Messaging solution that provides unified voice-mail, e-mail and fax-mail from a single highly-scalable mailbox architecture. DC-UniStore is available in both Service Provider and Enterprise-level configurations.

DC-UniStore comprises:

- a distributed, high-performance mailbox system, scalable to millions of mailboxes, which gives users a single repository for all message content types
- access via any POP-3 and IMAP-4 compliant clients (plus MAPI clients for the Enterprise-level solution), telephone, fax or Web browser.
- a unique telephony server that provides integrated telephone access to mailboxes, directory services, messaging services and web sites
- comprehensive backbone store-and-forward messaging support, including support for X.400, ESMTP/MIME, VPIM and AMIS profiles
- comprehensive management tools
- auditing/billing capabilities (Service Provider system only)
- a robust, distributed directory infrastructure including meta-directory connectors to legacy data, selective delegated administration, and open standards support for integration with other LDAP and X.500 directory services.

For more information on DC-UniStore, contact messaging@datcon.co.uk

SurroundSuite™

The SurroundSuite™ product family offers Unified Messaging solutions which combine Data Connection's best-of-breed datacomms and telecomms software products with leading industry messaging clients and servers, thus preserving an enterprise's current IT investments instead of introducing costly "forklift" solutions, or enabling Service Providers to supplement existing features and extend the range of outsourced services available.

The concept behind SurroundSuite™ is simple. In the age of open standards combined with rapid technological evolution, there is an overwhelming commercial need to evolve heterogeneous messaging environments rather than revolutionise them - both to avoid vendor shut-in, and to ensure that users can obtain new services in a timely and cost-effective manner.

The SurroundSuite™ product family is designed to provide both breadth and flexibility, and includes products for extending mailbox access, combining message types, gatewaying between message formats, and integrating multiple directory and provisioning environments, as well as unique Intelligent Agent features such as the ability to synchronise and manage a user's multiple mailboxes.

Any one product from the suite can be deployed in isolation to address a specific requirement, or multiple products can be combined to surround and embrace existing products and services in order to provide a comprehensive Unified Messaging environment.

For more information on SurroundSuite products for Service Providers, click here.

For more information on SurroundSuite products for the Enterprise, click here.

Core Messaging Solutions

For Service Providers and enterprises who are seeking a major upgrade to their core messaging infrastructure, Data Connection also delivers first-class messaging mailbox and store-and-forward servers, which can be deployed individually to upgrade core services, or in conjunction with the SurroundSuite™ products to provide a comprehensive solution.

- DC-Mailbox is a high-function, scalable multi-media Internet mailbox server, with unique software resilience features which make it ideal for deployment by Service Providers (SPs) and large enterprises. It can be fully packaged with Data Connection's other messaging products, or can be integrated with third-party client applications, backbone servers or directory systems.
- DC Integrated Messaging Server (DC-IMS) is a robust, scalable, store-and-forward messaging switch, which provides a complete solution for use in single and mixed-protocol messaging backbones.
- DC-Transport is a comprehensive product set for message-enabling existing communications products, providing a suite of application APIs and high-function ESMTP/MIME and X.400 protocol stacks.
- DC-VoiceNet is an extremely powerful platform for rolling out quality telephone-based information solutions, which provide access to existing messaging, directory, and web data from standard telephone handsets.

Expert Software Development Services

As well as our off-the-shelf solutions, Data Connection has a unique pool of software development expertise with which to assist our customers in the creation and deployment of their messaging solutions.

Read more about our work with some of our existing customers, and the reasons why our customers choose DCL to be their number-one choice as messaging technology supplier and partner.

For details of product Year 2000 conformance, download: Messaging Products Year 2000 Conformance Statement (Word 6 format).

For more information on our messaging software products and services, contact messaging@datcon.co.uk

Home
email: info@datcon.co.uk

STRATEGIC SOFTWARE TECHNOLOGY

Company
Products
Recruitment
Contact Us
Home
News

DC-Share for UNIX

DC-Share for UNIX is the first T.120 and H.323 data, audio and video conferencing product for UNIX that can interoperate with Microsoft's NetMeeting.

Conferencing
DC-Share for UNIX
- DC-Share FAQ
- Screenshots
DC-MeetingServer
Development Standards
Why DCL?

DC-Share for Linux Beta1 is now available - email dcsl@dataconnection.com.

DC-Share allows UNIX users to participate in conferences over the Internet and corporate intranets with Windows 95, Windows 98 and Windows NT users running NetMeeting, with UNIX users running DC-Share (available from Sun, SGI, and HP), and with users running other T.120 and/or H.323 compliant products from companies such as Netopia and PictureTel. Within the conference, DC-Share users can:

- view and control applications shared from Windows 95, Windows 98, Windows NT and other UNIX systems
- share local UNIX applications into the conference, which can then be viewed and controlled by other conference participants
- use the whiteboard, file transfer, chat and shared clipboard applications to exchange ideas and data
- talk to and see other conference participants.

DC-Share for UNIX includes:

- T.128 (formerly known as T.SHARE) application sharing
- T.126 and NetMeeting-interoperable whiteboards
- T.127 multipoint file transfer
- NetMeeting-interoperable chat and shared clipboard applications

- LDAP and NetMeeting ILS directory access
- T.120 MCS/GCC multipoint communications over TCP/IP
- H.323 audio and video, including multicast/multipoint video without requiring an MCU.

The DC-Share application sharing, whiteboard, chat and shared clipboard applications are based on the technology we developed for Microsoft's NetMeeting product.

The current version of DC-Share for UNIX is Release 3.0 which supports the full range of data, audio and video conferencing capabilities itemised above.

DC-Share for UNIX is available as part of Sun's SunForum, SGI's SGImeeting, and Hewlett-Packard's HP VISUALIZE CONFERENCE products. For other UNIX platforms, including AIX, please contact conf@dataconnection.com for details of availability. To find out how to download a free beta version of DC-Share for Linux, email dcsl@dataconnection.com.

DC-Share is primarily targeted at UNIX OEMs and vendors who wish to build T.120 and H.323 conferencing products that interoperate both with Microsoft's NetMeeting product and with other conferencing products that comply with the T.120 and H.323 series of conferencing standards.

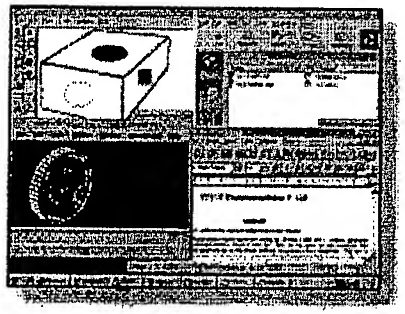
DC-Share is also available to large corporate end-users who wish to acquire and rollout a single NetMeeting-interoperable conferencing product across their complete range of UNIX platforms. Given Data Connection's focus on technology and engineering, we can only realistically provide a proper level of support to a small number of strategic end-users, where there is the prospect of a long-term relationship and/or there is a sufficiently large number of UNIX seats.

The screen shots below show a Windows NT system running NetMeeting 2.1 (on the left) and a UNIX system running DC-Share 2.1 (on the right) in a conference.

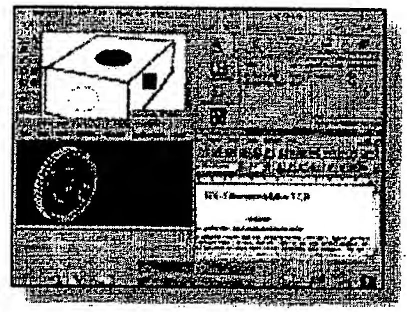
- The NetMeeting and DC-Share user interfaces are visible at the top right of the respective screens.
- The Windows user has shared Word into the conference - with the result that the UNIX user can view and control the shadow Word window as if it was running locally (even though it is actually running remotely on the hosting Windows system).
- The UNIX user has shared Pro/Engineer into the conference - with the result that the Windows user can view and control the Pro/Engineer 3D model as if it was running locally (even though it is actually running remotely on the hosting UNIX system).
- The users have also started whiteboards and have loaded up a simple drawing with annotations.

While the two screens are shown here side by side, in practice they might be very far apart (e.g. across the Atlantic), yet NetMeeting and DC-Share allow the users to collaborate irrespective of platform or location. Click on one of the screens to see it full size (800x600) and get more details.

Windows NT NetMeeting



UNIX DC-Share



DC-Share is portable to a wide variety of UNIX systems and hardware/display configurations. The product architecture isolates operating system and X server specifics to a small number of well-defined functions, which means that DC-Share for UNIX can normally be ported to a new UNIX environment with relatively little effort.

See the DC-Share Frequently Asked Questions (FAQ) for more information about DC-Share for UNIX or contact conf@dataconnection.com.

STRATEGIC SOFTWARE TECHNOLOGY

DATA CONNECTION

Company
Products
Recruitment
Contact Us
Home
News

DC-H.323

DC-H.323 is a server-class H.323 implementation capable of efficiently supporting large numbers of clients. It is much more than a protocol stack, incorporating video and audio media stream handlers and multi-party call control.

We expect DC-H.323 to appeal to hardware and software vendors seeking to produce reliable, high-performance H.323-compliant server products incorporating high-level handling of audio and video streams, while minimising their development risk.

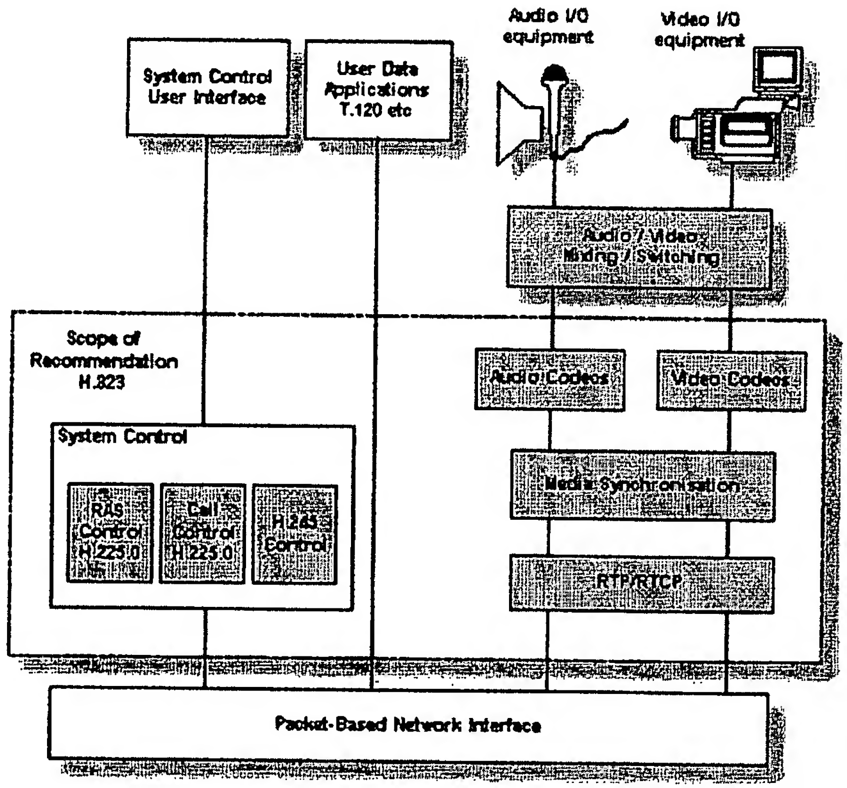
Conferencing
DC-Share for UNIX
DC-MeetingServer
- DC-MeetingServer Tour
- DC-T.120
- DC-H.323
- DC-WebShare
- DC-Recorder

Development Standards
Why DCL?

The H.323 Standard

H.323 is the ITU standard for audio and video conferencing over IP-based networks (including LANs and the Internet). As the diagram below shows, H.323 is primarily a grouping of separate standards for:

- call setup and management (Q.931 signaling, H.225.0, H.245)
- real-time data transfer (RTP, RTCP)
- audio/video encoding (G.711, G.723.1, H.261, H.263, etc).



A system implementing H.323 may have one, or sometimes several, of a number of different roles within the network - the key ones being:

- **Terminal**
  A regular or video "phone" like Microsoft NetMeeting
- **Gatekeeper**
  Responsible for control functions such as admissions, bandwidth allocation, address lookup, and call routing
- **Gateway**
  A converter between H.323 and other audio/video protocols such as H.320 (ISDN) and PSTN
- **MCU**
  Responsible for mixing audio and video - essential for most multiparty conferences.

DC-H.323 Overview

DC-H.323 implements the latest version (v2) of the H.323 standard, with:

- H.225.0 V2, which includes
  - RTP/RTCP
  - RAS
  - Q.931
- H.245 V3.

DC-H.323 also includes higher-level components for

- multi-party call control - a significant component which is not usually part of a "regular" H.323 protocol stack
- audio/video stream handling, including synchronisation and buffering
- audio mixing (which can be easily moved onto off-board DSP cards for increased scalability)
- video switching, based on either explicit control passing or automatic detection of who is speaking.

All components are extensively tested in client and MCU environments, and support multiple concurrent conferences and multiple nodes per conference. Particular emphasis has been placed on scalability, reliability performance and interoperability - we have conducted extensive interoperability testing with other H.323 implementations, both at the IMTC interoperability events and in bi-lateral testing using our own interoperability test lab.

High-level APIs enable OEM customers to integrate DC-H.323 easily within their own products. The particularly tricky problem of combining H.323 calls with T.120 conferences is hidden from the application programmer by the Conference Manager API, as used in DC-MeetingServer.

DC-H.323 Availability

DC-H.323 is a core component of DC-MeetingServer and of DC-Share for UNIX.

Data Connection does not supply the core H.323 stack as a standalone product, but works closely with its OEM customers to produce larger solutions based on DC-H.323 and other Data Connection technology. For example, our ATM and telecommunications experience means we are well placed to help our customers build gateways to ATM and SS7 networks using DC-H.323.

DC-H.323 is available now on Windows NT and 2000, as part of DC-MeetingServer.

Beyond Release 1, we closely follow developments in related standards processes and will add features (such as H.450 supplementary call services) as required by our customers.

For more information about Data Connection's conferencing products and expertise contact conf@dataconnection.com.

Home
email: info@dataconnection.com

DC-WebShare

DC-WebShare provides a mechanism for lite downstream clients to participate (through a T.128 Gateway running on a server) in T.128 application sharing sessions.

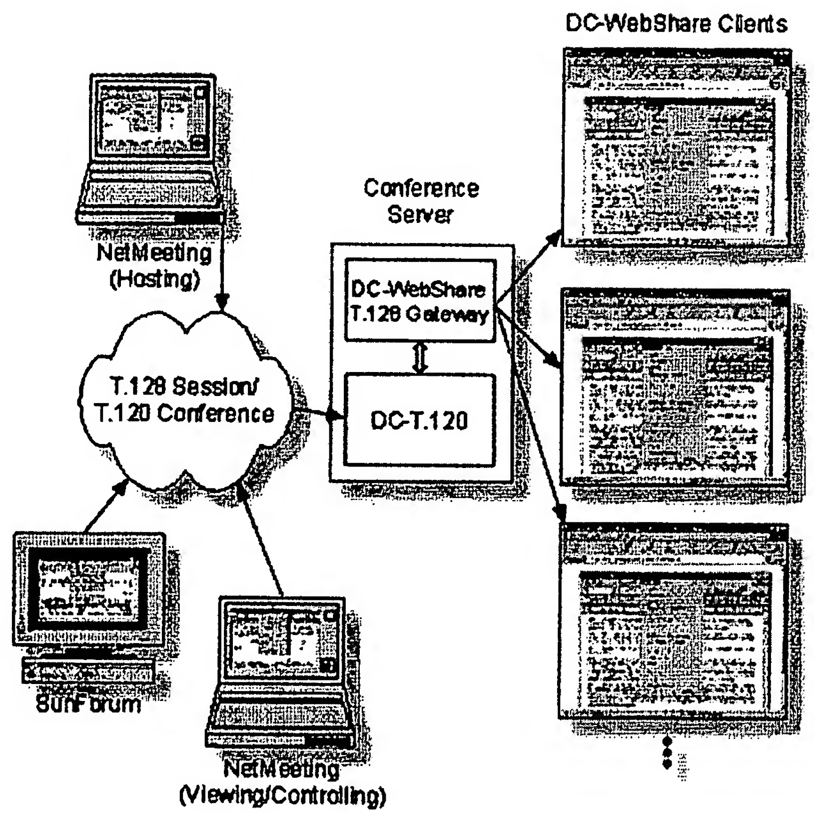
For example, users might use a browser to go to a conference URL (supplied in an email) and click on a link to enter the conference, whereupon they could view (and control) applications shared by NetMeeting within the browser.

DC-WebShare is in no sense a replacement for Microsoft's NetMeeting but it does provide an entry-level mechanism for end-users to participate in conferences and on-line presentations.

We envisage that infrequent conferees would use DC-WebShare as a way of participating in conferences without having to first install NetMeeting. But, as they start to conference more, they will want to install NetMeeting (or SunForum, SGImeeting, or HP VISUALIZE CONFERENCE) so they can share applications, use chat or the whiteboard or the other collaboration tools.

DC-WebShare consists of the following components:

- T.128 Gateway
- browser-embeddable downstream client.



DC-WebShare T.128 Gateway

The T.128 Gateway runs on a conference server (or similar) and participates in T.128 sessions within T.120 MCS/GCC conferences. It then forwards the application sharing session contents to downstream clients - so the end-users can view and/or control applications that have been shared from NetMeeting or SunForum.

The T.128 Gateway supports multiple concurrent upstream T.128 sessions (in multiple conferences) with multiple downstream viewing/controlling clients per concurrent session. Particular emphasis has been placed on scalability, reliability, performance in large

conferences and under heavy loads - and on interoperability with existing T.128 implementations, such as NetMeeting, SunForum, SGImeeting, HP VISUALIZE CONFERENCE, Timbuktu, and DC-Share.

Downstream clients do not appear in the GCC conference roster(s) - they are anonymous (which facilitates conference scalability). The T.128 Gateway provides an API whereby a local conference management program can retrieve information on connected downstream clients for display (say) in a web-based conference summary.

The T.128 Gateway can run on top of DC-T.120 or other T.120 MCS/GCC implementations. The latter case requires that the pre-existing T.120 MCS/GCC implementation:

- exposes the IMTC MCS/GCC APIs
- supports multiple concurrent conferences.

DC-WebShare Downstream Protocol

The downstream protocol between the T.128 Gateway and downstream clients is a private gateway/client protocol, which runs over TCP/IP or HTTP.

Running over HTTP enables gateway/client communication through standard firewalls without requiring specific firewall configuration changes.

DC-WebShare Client

The DC-WebShare Client is written in Java and executes as an applet or within a WWW browser - there is no requirement for installation. It is completely downloadable and has a download footprint of less than 50 Kbytes.

Client users can view and control applications hosted by other nodes within a conference, but cannot themselves share applications into a conference.

DC-WebShare Availability

DC-WebShare is available either as a standalone component, or as part of DC-MeetingServer.

DC-WebShare is being developed on both Windows NT and UNIX - although the DC-WebShare client (which is written in Java) is OS independent.

Release 1 of DC-WebShare is available on Windows NT during 1Q 99, with a UNIX version being available soon after. We expect to be able to make engineering (Beta) releases available to OEM partners prior to the final release.

For more information about Data Connection's conferencing products and expertise contact conf@dataconnection.com.

Home

email: info@dataconnection.com

DC-Recorder

DC-Recorder is to a conference what a VCR is to a TV broadcast. That is, it can make a real-time copy of the conference for later playback.

For example, a recording might be used:

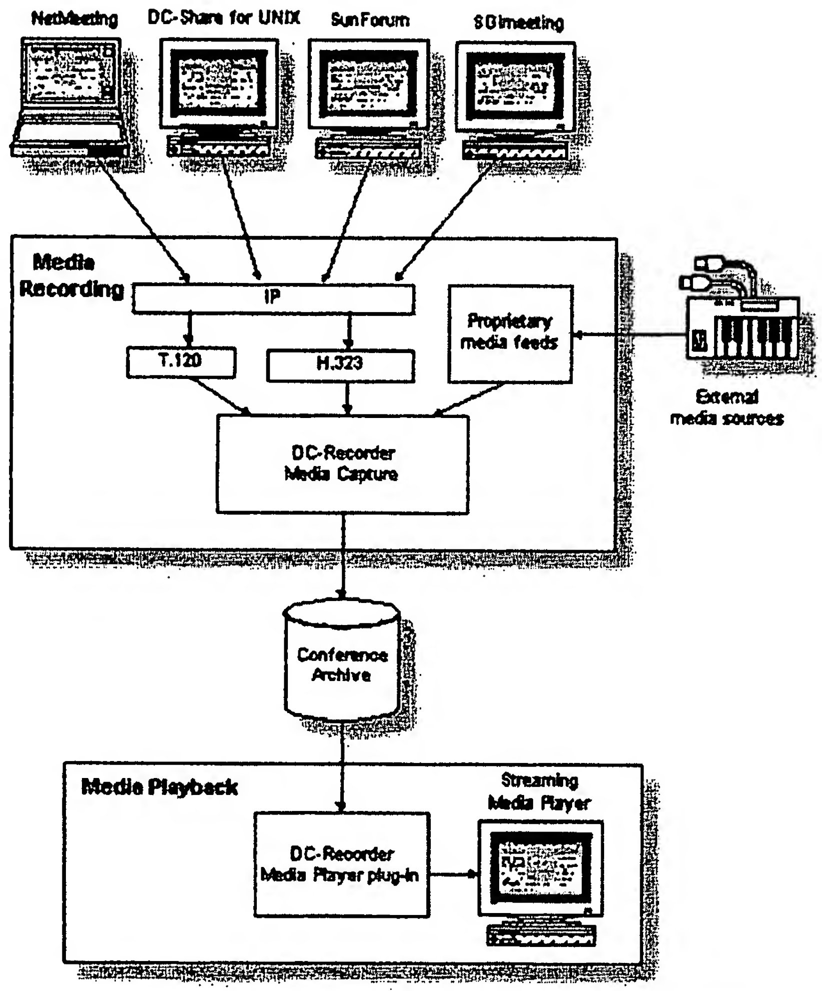
- as a briefing for people who were unable to attend the original conference
- as an easily prepared education session, showing the actual use of an application with an associated audio-visual commentary
- as a permanent record of a meeting in which important verbal decisions are made
- to satisfy requirements for making a formal archive of any conference that takes place.

Any conference participant can initiate the recording process simply by "inviting" a DC-Recorder system to join the conference. DC-Recorder will then join the conference and start capturing all recognised media formats. Examples of data that can be recorded are:

- H.323 audio and video streams
- Real-time display of any applications that are shared (for example by using Microsoft's NetMeeting)
- Real-time display of whiteboard contents
- Text from a Chat session
- Files transferred during a conference
- Any audio stream (A-law or u-law) or bitmap image that is fed into the DC-Recorder Media Recorder Interface.

DC-Recorder consists of the following components:

- Media Recorder
- Media Player plug-in for interpreting T.120 media streams
- User Interface applets for controlling recording.



DC-Recorder Media Recording

The Media Recording part of DC-Recorder records all supported media formats to a permanent storage device (hard disk, DVD-RAM or tape drive). Each media type is stored as a separate stream, with associated timing information for use when replaying the stream.

DC-Recorder Media Playback

Replaying a session simply involves feeding a recording into a streaming media player (such as the RealNetworks™ player or the DC-Recorder Player Java applet). The player determines which media streams are present and loads the appropriate DC-Recorder Media Player plug-in to interpret the conference media.

DC-Recorder User Interface

The DC-Recorder user interface is modelled on a simple VCR control panel. As you would expect, this supports functions such as play/record/stop and fast-forward/rewind.

The DC-Recorder UI provides functions for:

- Recording (record / pause recording / mark index)
- Playback (play / pause / rewind / fast-forward / jump to index point)

DC-Recorder Availability

DC-Recorder is available either as a standalone component, or as part of DC-MeetingServer.

DC-Recorder is being developed on both Windows NT and UNIX.

Release 1 of DC-Recorder supports:

- application sharing
- audio.

It will be available on Windows NT during 2Q 99, with a UNIX version being available soon after. We expect to be able to make engineering (Beta) releases available to OEM partners prior to the final

release.

Future releases of DC-Recorder will include support for other media types.

For more information about Data Connection's conferencing products and expertise contact conf@dataconnection.com.

Home
email: info@dataconnection.com

DC-MeetingServer

DC-MeetingServer is a packaged server product for standards-based conferencing. It is intended for use by:

- hardware and software vendors seeking to produce a full-function quality solution while minimising risk, development effort and time to market
- Internet and telecommunications service providers who want to offer value-add conferencing services
- large end-user organisations deploying conferencing technology.

Take a tour of a typical meeting using DC-MeetingServer.

The pre-integrated component technologies in DC-MeetingServer are also available for separate licensing by vendors looking to enhance their existing offerings such as MCUs, gateways, conference servers, Internet ACDs and other conferencing infrastructure products.

With DC-MeetingServer, Data Connection is harnessing an unrivalled range of experience and engineering skills.

- We developed the core data conferencing portions for Microsoft's NetMeeting on Windows.
- Sun's SunForum, SGI's SGImeeting, and Hewlett-Packard's HP VISUALIZE CONFERENCE are based on our DC-Share product, the first T.120 and H.323 conferencing application for UNIX.
- Our extensive experience in conferencing has enabled us to implement a set of unique value-add features that users are looking for, such as browser-based conferencing

through firewalls and conference recording.

- We know what is required, from both engineering and project management perspectives, to deliver high-quality, server-class technology - on time and for a fixed price. (See Why DCL? for more on our expertise in general.)

The rest of this page expands on the above with

- a discussion of conferencing today, and the need for a server-based conference infrastructure
- a summary of DC-MeetingServer features
- an overview of the DC-MeetingServer architecture
- information on availability.

The Need for Conference Infrastructure

Conferencing is now a critical business resource, with the proliferation of standards-based desktop clients that integrate audio, video and data within the organisation.

- Major US corporates are rolling out Microsoft's NetMeeting as part of their standard desktops to facilitate split-site group working, richer client meetings and distance training, to name just a few of the many applications of this technology.
- With products on Macintosh (Netopia), Sun Solaris, SGI IRIX, HP-UX, and other UNIX versions (DC-Share), standards-based conferencing is now available on all major desktop platforms.
- A recent Gartner study estimated that the number of active users of real-time document-sharing applications will increase from 200,000 in the first quarter of 1998 to at least 10 million in 2001.
- Conferencing is increasingly a major component of audio, video and/or data support in vertical markets, such as banking or retail kiosks.

While most desktop conferencing clients support ad-hoc point-to-point calling, the growth of desktop conferencing is currently limited by a lack of sufficient infrastructure support - whether inside the organisation or within the network backbone. A number of different considerations combine to make a server-based solution a clear requirement for universal, business-quality conferencing.

- **Bandwidth optimisation**
  Setting up conferences with a server can drastically reduce the volume of data traffic flowing, and substantially increase performance, in typical conferencing scenarios.
- **Ease of use**
  A conference server can act as a set of "meeting rooms", with easy-to-use web pages to locate and conference with other users.
- **Firewalls**
  Even where firewall products support conferencing protocols, it is usually simpler and more efficient to use a conference server as a bridge between separate domains.
- **Accessibility**
  Where conferences include users outside the organisation, a conference server such as DC-MeetingServer can provide conference access using regular web pages. This enables all users to participate, even without appropriately configured firewalls or conferencing applications.
- **Multiparty audio and video**
  Some conferencing clients only support multiparty audio and video conferences through a Multipoint Control Unit (MCU) which performs switching and/or mixing of audio and video. This function is typically part of a wider conference server product.
- **Administration and diagnostics**
  A network administrator might use a conference server to monitor and control usage and bandwidth, and solve user or network problems.
- **Security**
  Access to conferences can be restricted at the server by password and/or user-level authentication.
- **Billing**
  Where conferencing services are provided by a third party (for instance, by an Internet Service Provider), a server can maintain billing information.

These and related factors are driving the market requirement for conferencing infrastructure products.

DC-MeetingServer

DC-MeetingServer runs on Windows NT or UNIX systems and provides the full range of features required for effective conferencing.

Version 1.1 (available now) includes the following features:

- A simple yet powerful user interface, accessible from any web page.
- High-performance data conferencing with our server-class T.120 implementation, DC-T.120.
- Multi-point audio and video mixing/switching over DC-H.323, enabling any H.323 terminal (including NetMeeting) to participate seamlessly in multi-party conferences.
- The ability for anyone with no more than a web browser to participate in the same meeting as NetMeeting clients (or similar products such as SunForum) by
  - sharing locally-running applications so they can be viewed and controlled by other Web-based participants, or by NetMeeting users
  - viewing and controlling applications shared by other Web-based participants or NetMeeting users (see the DC-WebShare product description for more details)
  - exchanging text chat messages with other Web-based participants and NetMeeting users
  - listening to audio streamed from the H.323 conference
  - using the Web-based whiteboard to exchange ideas and graphics.

  These unique capabilities at last bring the benefits of conferencing to every user's desktop, even those located the other side of a firewall!
- Recording, archiving and playback of conferences with DC-Recorder. This
  - avoids laborious note-taking, enabling the meeting to flow more smoothly
  - provides a valuable recording for anyone missing the meeting
  - enables training/classroom sessions to be saved and re-used
  - facilitates automatic archiving of key decision-making meetings.
- Optional integration with existing enterprise and service provider user directories, by means of the DC-MetaLink directory synchronization module.

Version 1.2 adds

- support for Windows 2000
- improved user interface, including "one-click" instant meeting scheduling

Version 1.3 adds

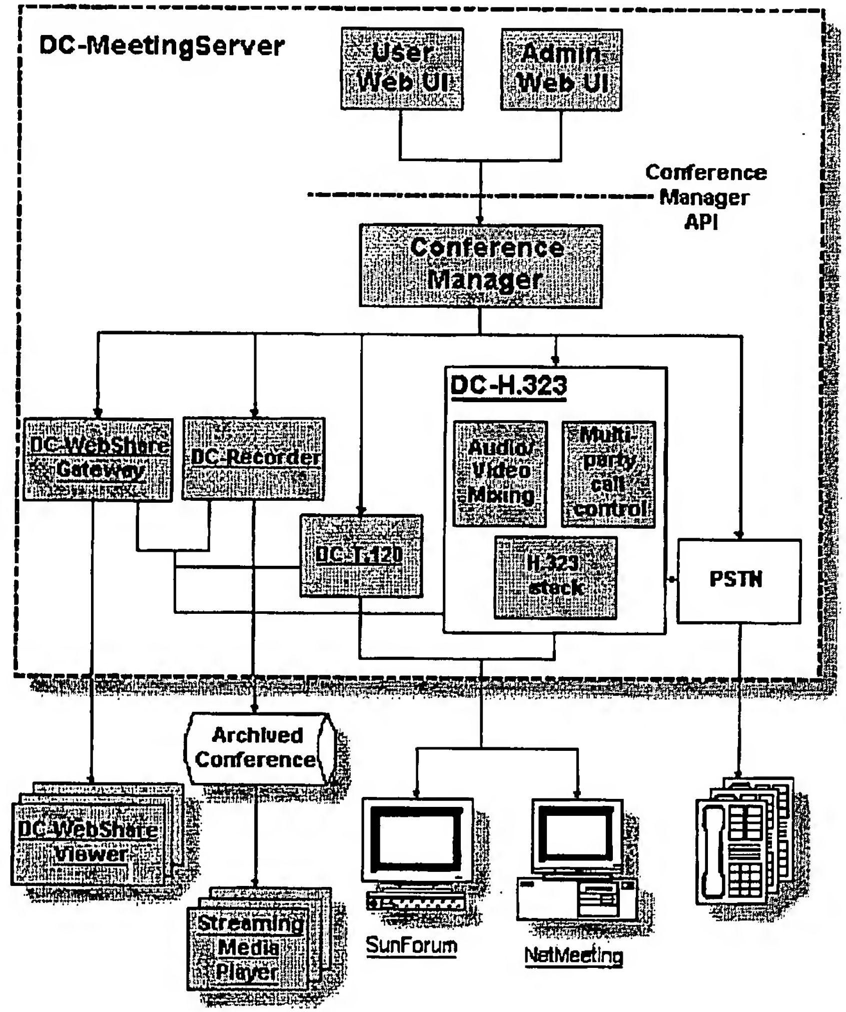
- a multi-page Web-based whiteboard, interoperable with NetMeeting
- enhanced Web-based audio features, including bi-directional audio, interoperable with NetMeeting and other H.323-based applications (including regular phones via an H.323 Gateway).

Version 2.0 includes the following features:

- Enhanced scalability and fault tolerance, including seamless scheduling across multiple systems, so that extending the number of supported users is simply a question of adding another DC-MeetingServer system. To the user, it simply appears as if a single server is supporting many thousands of clients.
- Support for Linux and Solaris platforms.

DC-MeetingServer Architecture Overview

The following diagram shows the components that make up DC-MeetingServer.



Particular emphasis has been placed on ensuring that DC-MeetingServer is ideally suited for easy customisation by OEMs and service providers, with the following features being built-in right from the system design phase:

- Modifiable web page templates, which make it easy to produce a unique look and feel to the system.

- Text-based configuration options to control most aspects of the system.
- For those needing to get involved at the source code level:
  - an easy-to-use high-level Conference Manager API, which hides the underlying complexity involved in tying together all the data, audio and video components
  - well-defined interfaces for each discrete component
  - extensive dynamically-filterable diagnostic, logging and tracing facilities.

DC-MeetingServer Availability

DC-MeetingServer version 1.1 is available on Windows NT today.

DC-MeetingServer version 1.2 is available on Windows NT and 2000 during 4Q 2000.

DC-MeetingServer version 1.3 is available on Windows NT and 2000 during 2Q 2001.

DC-MeetingServer version 2.0 is available on Windows NT / 2000, Linux and Solaris during 3Q 2001.

Data Connection reserves the right to alter product features and/or schedules. In particular, we are often able to consider increasing the priority of certain features, or implementing additional ones, in response to particular customer demands. Please contact us to discuss your requirements.

For more information about Data Connection's conferencing products and expertise contact conf@dataconnection.com.

Home

email: info@dataconnection.com

DC-MeetingServer

The real-time conferencing solution for Service Providers and large enterprises

DC-MeetingServer is a carrier-grade, high-function, conference server solution which allows Service Providers to deploy a robust, scalable, manageable web conferencing service including voice, video and data to consumers, enterprises and virtual ISPs.

DC-MeetingServer is also suitable for deployment directly within large enterprises that wish to have the closer control - and lower costs - that only a powerful, flexible in-house system can provide.

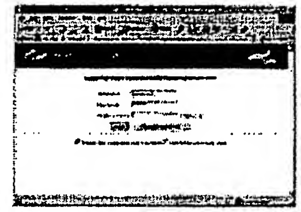
Conferencing Features

Key features of DC-MeetingServer include:

- easy-to-use, firewall-friendly **web conferencing** with high-performance application sharing, annotations, slide shows, whiteboard, chat, audio and video
- a powerful software-based **audio/video/data MCU** supporting NetMeeting and other H.323/T.120 clients
- **unique gateways** between H.323/T.120 and web conferencing, enabling browser-based clients and NetMeeting clients to participate fully in the same meeting
- a **scalable architecture** supporting thousands of concurrent conferences and millions of registered users on a single server farm installation

- Product Spec Sheet
  A summary of DC-MeetingServer's technical specifications
- DC-MeetingServer Product Description
  A more detailed description of DC-MeetingServer
- Web Tour
  A guided tour of DC-MeetingServer's web interface.

- ad hoc and advanced **conference scheduling** with iCalendar and Outlook integration
- a flexible, customisable UI suitable for **rebranding and co-branding** deployments
- **record and replay** of conferences
- a range of **security features** including encrypted conferences and restricted access conferences



- Live Demo Site!
  Try DC-MeetingServer for yourself

As with all of Data Connection's Internet Application solutions, DC-MeetingServer is built upon the following key infrastructures:

- our Unified Directory Platform, which includes
  - our scalable, distributed LDAP directory
  - flexible delegated administration with virtual ISP (wholesaling) support
  - single-point-of-provisioning for multiple services (e.g. messaging and conferencing)
- our Unified Management Platform, which includes
  - directory-based system configuration
  - sophisticated system reporting and management tools
  - integration with HP OpenView management consoles
  - single-point-of-administration for multiple services (e.g. messaging and conferencing).

Conferencing Technology

Data Connection has been the leading supplier of conferencing technology to the industry's OEMs and Service Providers since 1991, with our software used by Microsoft, PictureTel, IBM, Sun Microsystems, SGI, Cisco and Latitude, in products such as NetMeeting, SunForum and MeetingPlace.

This same technology is at the heart of Data Connection's packaged conferencing solution, DC-MeetingServer, which boasts the widest range of functionality and the highest performance of any conference server.

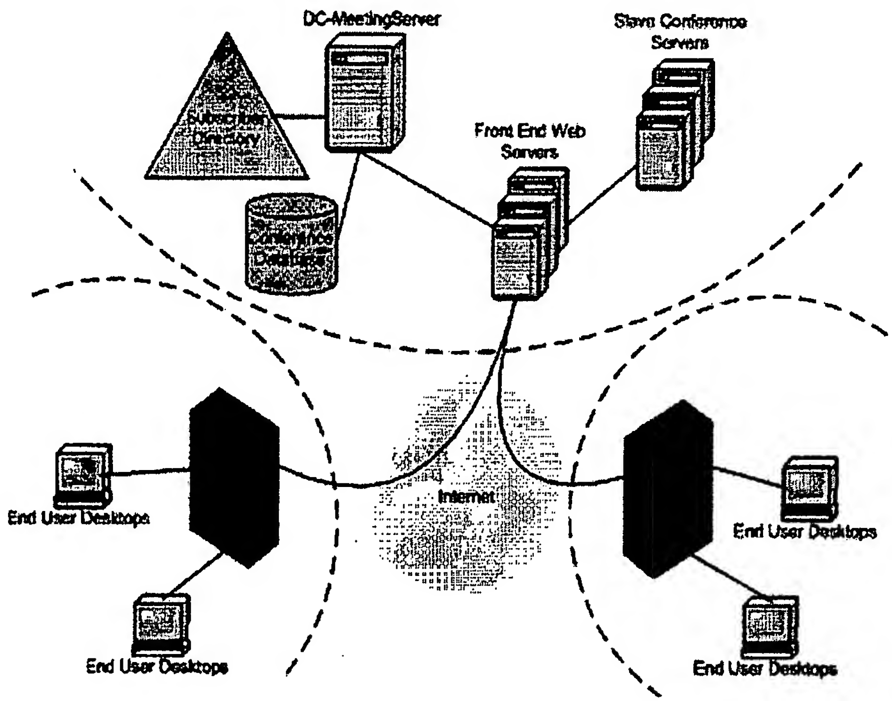
Since DC-MeetingServer is built upon our carrier-grade Unified Directory and Unified Management Platforms, it allows Service Providers to deploy a common architecture for conferencing, messaging,

directory and other web services - resulting in lower total cost of ownership through superior manageability and easier cross-selling of services.

Conferencing Architecture

DC-MeetingServer's architecture is optimised for large-scale Service Provider deployments, supporting 10,000s of simultaneous conferencing users (ports) - but is also available for entry-level single server systems supporting up to 500 ports.

The following diagram illustrates a distributed multi-server conferencing deployment based on DC-MeetingServer. All of the components shown within the Service Provider network are supplied as part of the DC-MeetingServer solution.



For more information about Data Connection's Internet Applications solutions, please contact

IAsolutions@dataconnection.com.

email: info@dataconnection.com

DC-VoiceNet Features

The following sections describe DC-VoiceNet's key differentiating features.

"Two for the Price of One" Publishing

If you already publish information electronically (on the Internet for example) you can now make it accessible from telephones and fax machines with virtually no extra overhead. DC-VoiceNet can present information from virtually any electronic media source including:

- Web pages from the Internet
- email messages from a corporate or ISP mail server
- online directories
- custom information direct from a network database.

Content Driven IVR

DC-VoiceNet eliminates the development work traditionally required to re-program IVR (Interactive Voice Response) systems when the structure or content of the data they publish changes. For example, if a Web page contains a list of links, DC-VoiceNet presents these as a menu of options to the user. If the Web page changes, the IVR menu automatically follows suit. DC-VoiceNet itself does not need to be modified in any way - it creates the user information dynamically in real-time.

Rich User Input

DC-VoiceNet processes user input by one or more of:

- detecting telephone key tones (often called DTMF)
- using speaker-independent speech recognition
- recording speech (for example dictated messages)
- receiving faxes (for example to be converted to an email).

Rich User Output

DC-VoiceNet presents user output using speech synthesis or pre-recorded digital audio sound files, or by sending faxes. Sound files may be:

- installed during DC-VoiceNet configuration: for example, standard menus can be "spoken" instead of synthesised
- provided as part of any data source: for example, a Web page can reference a set of sound files to use in preference to speech synthesis, to represent some or all of the text on the page - or even to play "jingles".

Telephony Functions

In addition to receiving and placing calls, DC-VoiceNet can also connect calls together, for example to connect users to a live operator on request at any time. When their call with the operator ends, users reconnect to DC-VoiceNet from the point at which they started talking to the operator.

Scalable to Meet Growth in Demand

DC-VoiceNet is capable of running on a single standalone PC to provide a small-scale service. More typically, DC-VoiceNet runs on a cluster of networked industrial PCs. It spreads the extensive telephony, data management, billing, diagnostics and auditing functions across the cluster using a scalable and fault tolerant architecture. Each node in the cluster can typically process around 60 concurrent telephone calls, with no theoretical limit to the number of nodes.

High Availability / Fault Tolerance

The DC-VoiceNet design supports true 24x7 operation if needed. Fault localisation is inherent in the architecture; for example, if a single node experiences a hardware failure, the other nodes in the cluster

- isolate the fault
- re-route processing as necessary
- continue functioning as normal.

Telephony Hardware and Engine Independence

Telephony and speech technology is advancing fast. DC-VoiceNet has been designed to take advantage of this from the outset. Clear boundary interfaces allow DC-VoiceNet to use different telephony hardware and speech engines with the minimum of effort. This means it can take advantage of state-of-the-art engines or satisfy particular customer preferences. To give an idea of its flexibility, DC-VoiceNet has been integrated with various components from Dialogic, Lucent, Digital, Centigram, Lernout & Hauspie, and Nuance.

Value Add Extensions

All of the features above come "out of the box", but DC-VoiceNet also allows you to develop customised add-on applications, offering services that are specifically targeted at your customer needs, and tuned to be "telephone aware". DC-VoiceNet supports this through:

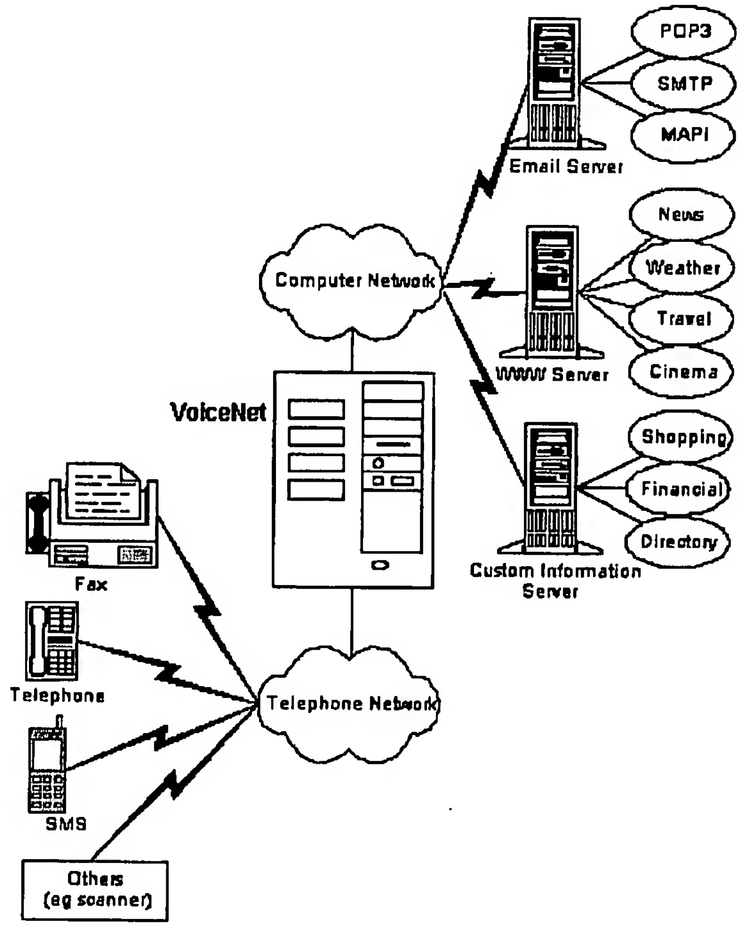
- ☐ DC-VoiceNet specific HTML extensions (which can be used on any Web pages you write, including Active Server Pages if complex processing is needed)
- ☐ exposing COM APIs to allow custom program access to DC-VoiceNet functions.

Home
email: info@dataconnection.com

DC-VoiceNet

DC-VoiceNet provides flexible access to information on the Internet/Intranet using standard or mobile telephones or faxes.

DC-VoiceNet is a combination of hardware (such as PRI-ISDN interface cards and rack mounted industrial single board computers) and software (such as information routing and processing, billing, and speech synthesis technologies).



With DC-VoiceNet, you can take data previously only accessible using networked computers, and make it available for browsing from any telephone world-wide - no special terminal equipment is required.

- A DC-VoiceNet user dials a telephone number associated with a DC-VoiceNet system, which accesses a "home page" for each user.
- DC-VoiceNet "reads" the contents of the Web page to the user by means of synthesised speech and/or pre-recorded sound.
- Hypertext links to other pages are identified in the audio output, and the user can select

and follow a link using telephone keys or spoken words.

- As well as Web pages, users can listen to their incoming email messages, and forward them or reply to them.
- DC-VoiceNet converts Web contents or emails into audio output in real time, without requiring any special processing in the HTML source. This means that you can use all your existing source information without any need to rewrite it for DC-VoiceNet.
- Users can follow links from the DC-VoiceNet "home page" to anywhere on the Internet; you are not restricted to DC-VoiceNet specific pages.
- As well as audio output, DC-VoiceNet can also send data to a fax machine.
- Pages can be set up to contain DC-VoiceNet enabled telephone numbers (for example in a corporate directory listing, or to provide a "more information" service). In this case, users can start a telephone call (or send a fax or voicemail message) direct to these numbers from within DC-VoiceNet.

DC-VoiceNet adds to on-line information services, giving them a low cost way to provide

- ubiquitous access - anyone with a standard telephone can now use the service
- enhanced function.

For more information on DC-VoiceNet features, see Features.

Application Areas

DC-VoiceNet is an extremely powerful platform for rolling out quality telephone-based information solutions that can easily adapt and expand as requirements change. It can be used in a number of different application areas, such as:

- Universal messaging for email, voice and fax
- Retail and home shopping
- Traffic reports
- Financial information
- Corporate directory access
- Directory enquiries / Yellow Pages

For more information on typical applications, see Applications.

Data Connection is also building full-function IP Telephony Gateway solutions, which integrate some of its key technologies, including H.323 audio and video, SS7 signalling, ATM, T.120 data conferencing, and directories. Using this, DC-VoiceNet users can access IP telephony. For more information on these associated technologies, see Conferencing Products.

In summary, DC-VoiceNet's flexibility and industrial strength architecture make it perfectly positioned to provide commercially compelling solutions across a very broad range of markets. In many cases, it uses existing information available from the Internet or an Intranet without modification - and therefore at very low cost. As the surrounding technology continues to evolve, DC-VoiceNet is ideally placed to take advantage of the best the industry has to offer, such as new speech engines, fax solutions, and hardware enhancements.

For more information about DC-VoiceNet and related products, contact dcvoicenet@dataconnection.com.

Home
email: info@dataconnection.com

Data Connection Home Page

STRATEGIC COMPUTER TECHNOLOGY

CONNECTION

Company
Products
Recruitment
Contact Us
Home
News

Messaging Software Products and Services

Messaging
DC-UniStore
SurroundSuite for Service Providers
SurroundSuite for Enterprises
Core Messaging Solutions
Customers
Why DCL?

Data Connection supplies a comprehensive range of messaging software products which have already been adopted in a wide range of services and solutions in the messaging industry.

- Product vendors employ our software within their messaging server solutions to provide high-function industry-standard message protocol support.
- Service Providers and large end-user organizations use our software to build high-end message backbone infrastructures.
- Systems Integrators use our technology and engineering expertise to help them create unique messaging solutions to address complex client requirements.

Using our unique portable software product architecture, Data Connection's messaging products are available on a wide range of platforms, including Solaris, HP-UX, AIX, and Windows NT ®.

Unified Messaging Solutions

Data Connection has a unique breadth of software expertise that spans both the data communications and telecommunications marketplaces. This enables us to provide a comprehensive range of products which provide Unified Messaging solutions.

DC-UniStore

DC-UniStore is a complete Internet-based Unified Messaging solution that provides unified voice-mail, e-mail and fax-mail from a single highly-scalable mailbox architecture. DC-UniStore is available in both Service Provider and Enterprise-level configurations.

DC-UniStore comprises:

- a distributed, high-performance mailbox system, scalable to millions of mailboxes, which gives users a single repository for all message content types
- access via any POP-3 and IMAP-4 compliant clients (plus MAPI clients for the Enterprise-level solution), telephone, fax or Web browser.
- a unique telephony server that provides integrated telephone access to mailboxes, directory services, messaging services and web sites
- comprehensive backbone store-and-forward messaging support, including support for X.400, ESMTP/MIME, VPIM and AMIS profiles
- comprehensive management tools
- auditing/billing capabilities (Service Provider system only)
- a robust, distributed directory infrastructure including meta-directory connectors to legacy data, selective delegated administration, and open standards support for integration with other LDAP and X.500 directory services.

For more information on DC-UniStore, contact messaging@dataconnection.com.

SurroundSuite™

The SurroundSuite™ product family offers Unified Messaging solutions which combine Data Connection's best-of-breed datacomms and telecomms software products with leading industry messaging clients and servers, thus preserving an enterprise's current IT investments instead of introducing costly "forklift" solutions, or enabling Service Providers to supplement existing features and extend the range of outsourced services available.

The concept behind SurroundSuite™ is simple. In the age of open standards combined with rapid technological evolution, there is an overwhelming commercial need to evolve heterogeneous messaging environments rather than revolutionise them - both to avoid vendor shut-in, and to ensure that users can obtain new services in a timely and cost-effective manner.

The SurroundSuite™ product family is designed to provide both breadth and flexibility, and includes products for extending mailbox access, combining message types, gatewaying between message formats, and integrating multiple directory and provisioning environments, as well as unique Intelligent Agent features such as the ability to synchronise and manage a user's multiple mailboxes.

Any one product from the suite can be deployed in isolation to address a specific requirement, or multiple products can be combined to surround and embrace existing products and services in order to provide a comprehensive Unified Messaging environment.

For more information on SurroundSuite products for Service Providers, click here.

For more information on SurroundSuite products for the Enterprise, click here.

Core Messaging Solutions

For Service Providers and enterprises who are seeking a major upgrade to their core messaging infrastructure, Data Connection also delivers first-class messaging mailbox and store-and-forward servers, which can be deployed individually to upgrade core services, or in conjunction with the SurroundSuite™ products to provide a comprehensive solution.

- DC-Mailbox is a high-function, scalable multi-media Internet mailbox server, with unique software resilience features which make it ideal for deployment by Service Providers (SPs) and large enterprises. It can be fully packaged with Data Connection's other messaging products, or can be integrated with third-party client applications, backbone servers or directory systems.
- DC Integrated Messaging Server (DC-IMS) is a robust, scalable, store-and-forward messaging switch, which provides a complete solution for use in single and mixed-protocol messaging backbones.
- DC-Transport is a comprehensive product set for message-enabling existing communications products, providing a suite of application APIs and high-function ESMTP/MIME and X.400 protocol stacks.
- DC-VoiceNet is an extremely powerful platform for rolling out quality telephone-based information solutions, which provide access to existing messaging, directory, and web data from standard telephone handsets.

Expert Software Development Services

As well as our off-the-shelf solutions, Data Connection has a unique pool of software development expertise with which to assist our customers in the creation and deployment of their messaging solutions.

Read more about our work with some of our existing customers, and the reasons why our customers choose DCL to be their number-one choice as messaging technology supplier and partner.

For details of product Year 2000 conformance, download: Messaging Products Year 2000 Conformance Statement (Word 6 format).

For more information on our messaging software products and services, contact messaging@dataconnection.com.

Home
email: info@dataconnection.com

Data Connection Home Page

STRATEGIC COMPUTER TECHNOLOGY

CONNECTION

Company
Products
Recruitment
Contact Us
Home
News

DC-SurroundSuite for Enterprises

The SurroundSuite™ product family offers Unified Messaging solutions which combine Data Connection's best-of-breed datacomms and telecomms software products with leading industry messaging clients and servers.

A key requirement for enterprises is how to evolve the messaging infrastructure to a comprehensive Unified Messaging strategy without having to deploy a complete "Forklift" solution, which is often untenable from both capital cost and user-disruption perspectives. The SurroundSuite™ product family offers a solution to this problem by providing a comprehensive range of products that can be used selectively or in combination, to enhance the existing corporate messaging infrastructure without demanding replacement of existing legacy systems.

Messaging

DC-UniStore

SurroundSuite for Service Providers

SurroundSuite for Enterprises
- DC-SurroundStore
- DC-SyncroMail
- DC-IMS\Voice
- DC-Directory
- Solutions for Microsoft Environments

Core Messaging Solutions

Customers

Why DCL?

DC-SurroundStore

DC-SurroundStore can integrate with an enterprise's existing mailbox systems to unify voice-mail, e-mail and fax communications in order to deliver a comprehensive single-mailbox solution for the user community.

Message browsing, send/reply, forwarding, and message management are available from PCs and/or touch-tone phones, regardless of message origin and format. Features include text-to-speech conversion, single-interface administration, LDAP/X.500 directory support, and fax-mail services.

DC-SurroundStore for Enterprises provides far more than "just" telephone access to mail. For example:

- The telephony server component within DC-SurroundStore enables telephone users to browse through available directory services, obtain details of entries, auto-connect their phone calls, send e-mails, voice-mails or faxes, and even browse their favourite public

web-sites (e.g. for weather reports, share prices) or hosted Intranets (for corporate data).

- An integrated H.323 server enables direct voice and data communications over the IP infrastructure, thus future-proofing the enterprise with an integrated Voice over IP service for messaging access.
- DC-SurroundStore can connect to multiple different groupware systems (e.g. Exchange, Notes, Netscape) and provide a consistent degree of Unified Messaging functionality across all these user communities.
- Using the unique web-based IVR system within DC-SurroundStore, an enterprise-specific range of phone-accessible applications can be made accessible for the user community that can improve data flow around the organisation and empower users with greater productivity.

For more information on DC-SurroundStore, contact messaging@dataconnection.com.

DC-SyncroMail

DC-SyncroMail is designed to address a key issue in Unified Messaging - how do you cope with environments where users each have multiple mailboxes? For example:

- The enterprise may not yet be in a position to offer a combined e-mail and voice-mail service in one mailbox, and thus needs an interim solution that provides some level of user-controlled management of the multiple mailboxes.
- A user may wish to have the data from his or her residential mailbox (or mailboxes) integrated and accessible via the corporate messaging service.
- The enterprise needs to be able to offer migration services to users of legacy messaging systems, in order to facilitate the migration to newer, more strategic products.

In all these situations, the ease-of-use of a single unified mailbox is simply not available. This is where DC-SyncroMail comes in.

DC-SyncroMail acts as an Intelligent Agent server for a user community, where each user can register personalized rules for how to manage a collection of his or her own mailboxes. Features include:

- selective forwarding of new mail to other mailboxes (including content conversion as

appropriate)

- automatic update of message status for duplicate mails in different mailboxes (read-status, deletions, etc)
- priority notifications (e-mail, voice-mail, cellular, pager)
- synchronised folder management
- hierarchical defaults and delegated administration.

In summary, DC-SyncroMail has no place in the idealistic world of single-instance universal mailbox and global directories, but is designed to address major issues to do with the reality of providing Unified Messaging services in a non-unified world.

DC-SyncroMail is available later in 1999. For more information, contact messaging@dataconnection.com

---

DC-IMS\Voice

DC-IMS\Voice is a standalone Universal Messaging backbone gateway which employs industry-standard voice and data protocols such as VPIM, AMIS and SMS to connect existing VoiceMail Systems with the Internet, desktop messaging systems, and wireless networks.

For more information on DC-IMS\Voice, click here.

DC-Directory

DC-Directory is a complete directory solution which combines the best elements of X.500 and Internet standards (LDAP, HTTP) with comprehensive management and administration applications to provide an open, scalable directory service for service providers and large enterprises.

In the context of Unified Messaging, DC Directory provides a complete directory infrastructure for provisioning and administration, including delegated authority, meta-directory connectors to legacy databases, and support for e-mail and voice-mail directory services.

However, the applicability of DC Directory goes far beyond Unified Messaging. DC Directory can provide a complete electronic directory infrastructure for a full range of services, including conferencing, E-commerce and Public Key security services.

For more information on DC-Directory, click here.

Solutions for Microsoft Environments

For an Enterprise environment, Microsoft products such as Windows NT/2000, Exchange, Active Directory and NetMeeting are becoming key products in many organisations.

Data Connection has enjoyed a long-term relationship as a core technology provider to Microsoft since 1987, and this relationship enables Data Connection to offer a unique range of solutions which complement core product offerings from Microsoft, including a packaged set of SurroundSuite™ products tailored specifically to enterprises that employ Microsoft products.

For more information on solutions for Microsoft environments, click here.

Core Messaging Solutions

For enterprises who are seeking a major upgrade to their core messaging infrastructure, Data Connection can also deliver first-class messaging mailbox and store-and-forward servers, which can be deployed individually to upgrade core services, or in conjunction with the SurroundSuite™ products to provide a comprehensive solution.

For more information on Data Connection's Core Messaging products, click here .

Home
email: info@dataconnection.com

SmartDialer

Functional Overview

Version v1.0

Internet Applications Group
Data Connection Limited
100 Church Street
Enfield
EN2 6BQ
United Kingdom

DATA CONNECTION

Table of contents

1 Overview

The way people use phones is changing. Broadband is becoming the norm. The backbone network is consolidating voice and packet data. New VoIP services are bringing call costs ever lower. Mobile devices are replacing or augmenting landline phones.

This changing landscape raises critical questions for the "traditional Telco".

- How do you take a large user base forward to the next generation of revenue making services?
- How can you leverage instant messaging and presence?
- What value can you add to a phone call?
- Where is your revenue going to come from when all calls are essentially free?

SmartDialer is part of Data Connection's response to those questions and provides a means for Telcos to add value and provide new services for their customer base.

SmartDialer comprises

- a Windows-based application targeted at home and business broadband users who are using both their PC and phone
- a SmartDial Server that resides in the Telco's network and enables many of the services.

The Windows applications is packaged as a base application that a Telco may provide at low cost or for free (for example as a download) that provides basic softphone function. Users can then upgrade (typically by paying an upgrade fee) to get additional value-added services on top of the basic offering.

The basic softphone features provided by SmartDialler are as follows.

- A PC-based endpoint for making and taking phone calls.
- Integration with other PC-based softphones.
- Control of traditional phone handsets.
- Call logging and history.
- Notification of inbound calls.

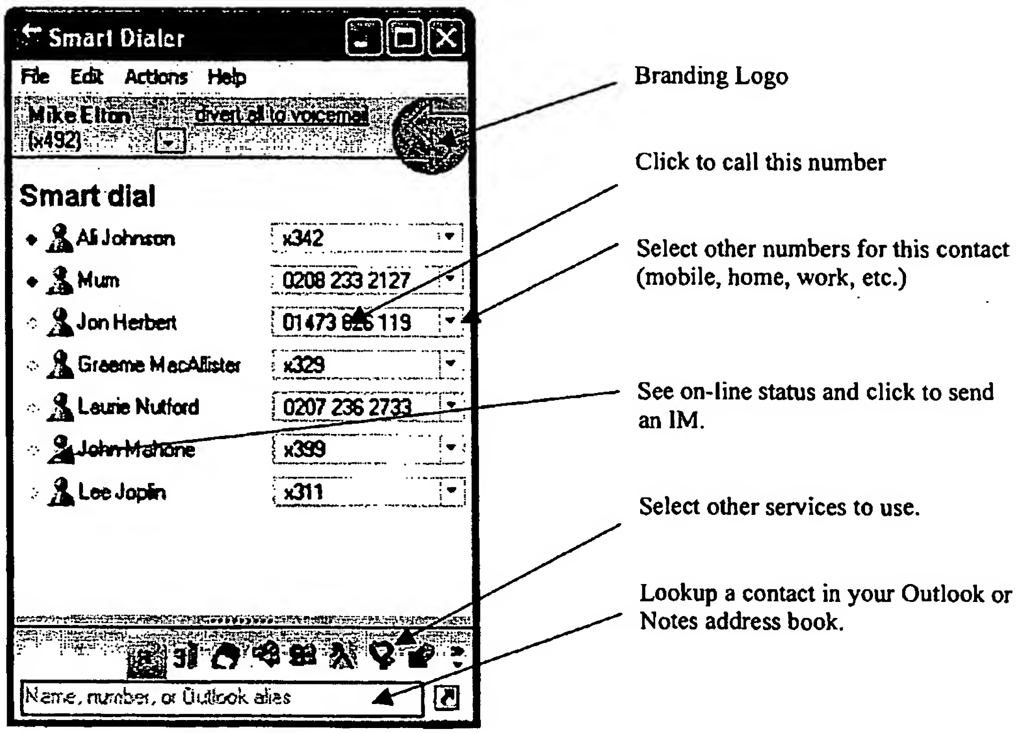
Additional services can be provided by the Telco and installed by the user simply by downloading them from the Telco's website or selecting them from with SmartDialer itself. SmartDialer has open APIs which can be used to add new features as required. The features incorporated in the first release of SmartDialer are

- Voicemail
- Audio and Data Conferencing
- White and Yellow pages integration
- Point-to-point Web and application sharing
- Video
- SMS Text, Picture and Video messaging.

1.1 Brandable and Extensible User Interface

The user interface for SmartDialer is designed to be intuitive and take up minimal real estate on a user's desktop. It can also be branded by the Telco to include suitable graphics and advertising.

The UI can also be extended with new services which can be downloaded by the user. For example, a user may have the basic click-dial service but want to buy voicemail from the Telco. All they need to do is select the option to "Add Voicemail" and from within the client they will be taken through the sign-up process and then be able to access voicemails from within SmartDialer.



Additional panes in the UI can be added either by the Telco, or by other service providers the Telco has a commercial relationship with. These are also available from the main GUI and can be added and removed by the user.

SmartDial makes adding these new services easy for a service provider whilst offering a high degree of customizability

2 SmartDialer as a Softphone

In its basic form, SmartDialer can operate as a softphone, integrated with a user's desktop, providing normal softphone capabilities:

- choice of using desktop VoIP phone or normal phone
- call history and logging
- notification of incoming calls.

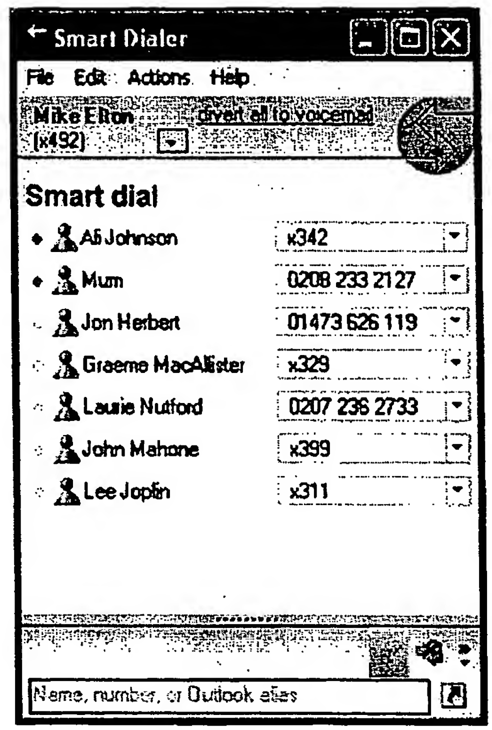
Where SmartDialer differs from other other products on the market is that it is built to be extended to provide other services on top of the basic features. These value add services are described in the next section.

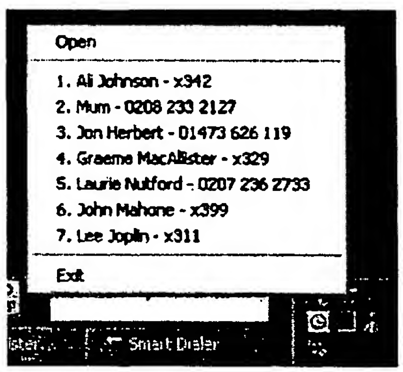
2.1 Smart Dial

The SmartDial is the core of the product. It presents a one-click route for those contacts that are most likely to be called.

The SmartDial list will choose the most likely phone numbers the user will want to use. However, if another number is available for the contact, the user can choose them via a drop-down control.

If an Instant Messaging client is installed on the users machine, and a contact matches one of these IM buddies, then the SmartDial list will show the current status of that person.



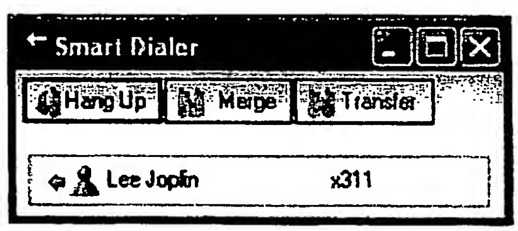


SmartDial contacts are also available from the system tray

2.1.1 Call Window

The call window describes the current call, including the call number and the contact name if available.

The call window automatically pops up when a call is placed or received from SmartDialer. It can also be configured to appear when the desk phone makes or receives a call.



Depending on the backend functionality and whether or not the user has two lines, it supports

- 3-way calling
- transfer call
- hang-up.

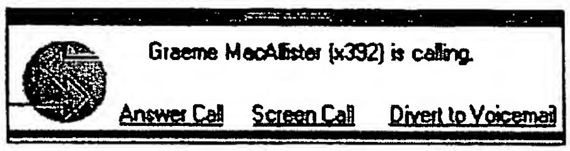
Additional information can be offered in the Call Window – services such as DataShare or Video connection, if these are available in the current call.

2.1.2 Incoming Call Notification

When a call is received, a popup is displayed giving the number that is calling and if it can be resolved, also the contact name.

The user then has the following options

- to divert the user to voicemail
- screen the call (by listening to the message on the PC speakers while the caller leaves a message on voicemail and then optionally pick the call up)
- answer the phone.



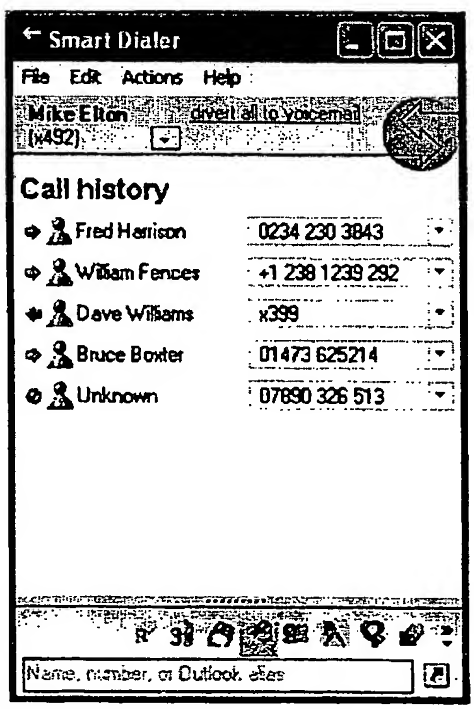
Inbound calls can also be managed using rules to, for example, forward all calls straight to voicemail except if they are from your boss, etc.

2.2 Call History

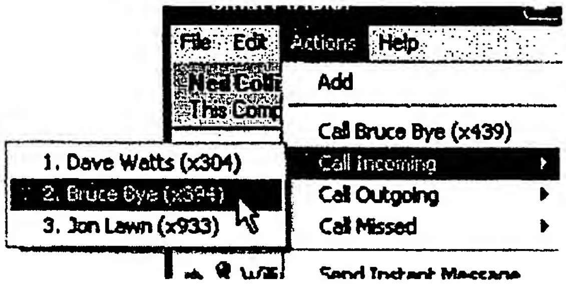
One of the goals of SmartDialer is to enable calls to be placed as easily as possible (so making more calls happen and increasing call volumes). A key part of this is the call history that is maintained by SmartDialer.

[Note that this information is obtained from the network but then stored locally. It will, therefore, also record calls dialed directly from the phone as well as those initiated from SmartDialer.]

By default the Call History shows all received, dialed, and missed calls, ordered by date order. The tool tip shows the date and time of those calls. It takes only one click to call that number.



To access the last 10 received, dialed and missed calls swiftly, it is also possible to get to these via the Actions menu.



The user chooses how long the history is stored for, and can also choose to view the Call History ordered by contact, as well as by date.

2.3 Desktop Integration Add-ins

SmartDialer integrates with other Windows desktop applications to leverage two kinds of functionality.

Workgroup applications

SmartDialer integrates tightly with the Microsoft Outlook and Lotus Notes to obtain contact details, including telephone numbers.

Instant Messaging

SmartDialer uses the user's preferred instant messaging application (Windows Messenger, Lotus Instant Messaging, Yahoo Messenger, AOL Instant Messenger and ICQ) to

- display presence information about the user's buddies in the SmartDialer user interface
- provide a means of sending an instant message to a buddy with whom the user is conducting a telephone call.

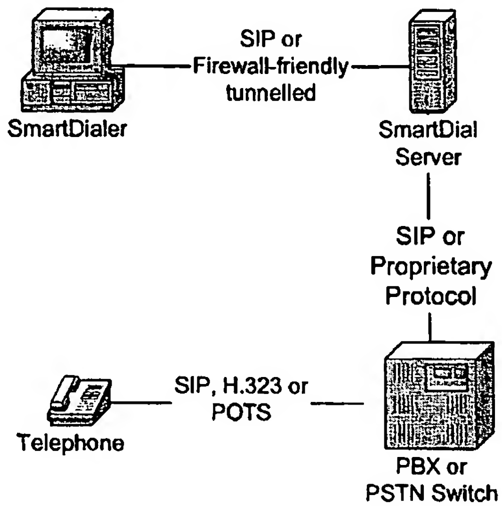
VoIP Clients

SmartDialer allows the user to choose between using their desktop traditional phone or a VoIP endpoint on their PC.

The user does not need to configure which VoIP application to use. Instead, SmartDialer periodically checks what VoIP phones are installed that it supports and adds these to the list of phones that can be controlled by SmartDialler.

2.4 Network Integration

The protocols used by SmartDialer for setting up calls are illustrated below.



SmartDialer to SmartDial Server	This protocol is either SIP (by preference) or a proprietary firewall friendly protocol (used if SIP is blocked by the network).
SmartDial Server to PBX/PSTN	This protocol is again SIP by preference (using either 1st or 3rd party call control). It can, however, be modified to use other protocols (such as CSTA, JAIN or Parlay).
PBX/ PSTN to Phone	The protocol between the PBX or PSTN and the regular phone is unchanged. If SmartDialer is being used as the endpoint then SIP is used.

SmartDialer is designed to be downloaded, installed and then "just run". This requires it to be very flexible in how it works with the network and that it can discover as much as possible automatically.

Step 1 - Discover PC capabilities.

- Once installed (and periodically thereafter) SmartDialer scans the local PC if installed applications it can run with (VoIP phones, group applications and Instant Messaging applications).

Step 2 - Discover network capabilities

- SmartDialer then works out if it is on a network which has a PBX and, if so, whether it can control it.

- If SmartDialer cannot find a PBX, it connects to the public network.

In both cases SmartDialer is trying to find a SmartDial Server which will manage the protocol interaction with the client and gateway to the phone network (either a PBX or the PSTN switches).

Step 3 – Determine Protocols to use

- Once SmartDialler has found a SmartDial server it then tries various protocols find out what protocols it can use to talk to the server. These range from SIP (which is the preferred mechanism and gives the best function and performance) through to using a proprietary protocol which is firewall friendly.

Step 4 - Phone Registration

- Once SmartDialer is communicating with its server it checks whether it has any phones registered with this server.
- Once connected the user can either use the SmartDialer to make calls as a VoIP endpoint or, optionally, register other phones to use.
- If the user chooses to register a different phone (for example their desktop phone), SmartDialer gives them a phone number to call and a PIN code to type in.

Once the above steps are complete, SmartDialer can start to establish calls.

3 Value Added Services

While the basic softphone features listed above are intended to gain interest from users and allow for rapid uptake of a Telco's SmartDialer offering the following features are intended for revenue generating services.

- Voicemail
- Audio and Date Conferencing
- Integration with White and Yellow pages services.
- DataShare services
- Video
- Text, picture and video messaging

3.1 Voicemail

The Voicemail service in SmartDialler uses IMAP-4 to access a Telco hosted voicemail system.

The voicemail feature of SmartDialler provides

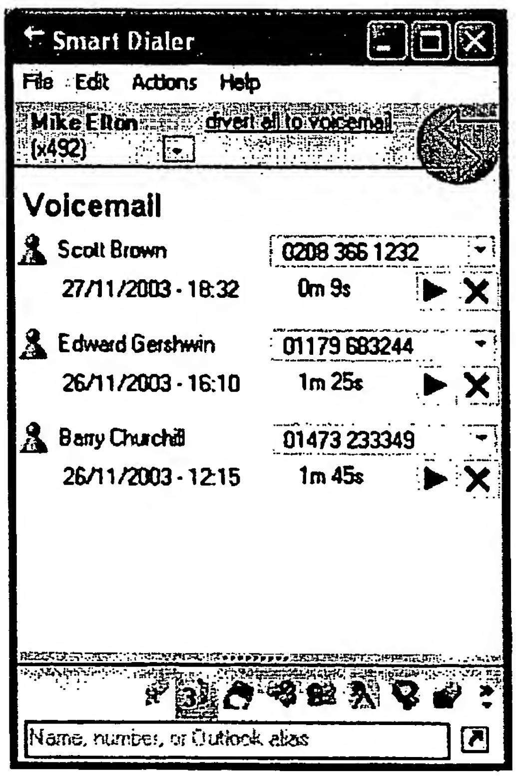
- name of caller (if available)
- phone number
- date/time
- caller IM status (if available)
- voicemail duration.

It also offers the following capabilities

- call the person
- play the voicemail (through your PC speakers)
- delete the voicemail.

The voicemail feature may also be configured to

- display notification when a voicemail is received
- display an icon in the system tray when unheard voicemails are present
- allow on-line sign up for a voicemail service.



3.2 Audio and Data Conferencing

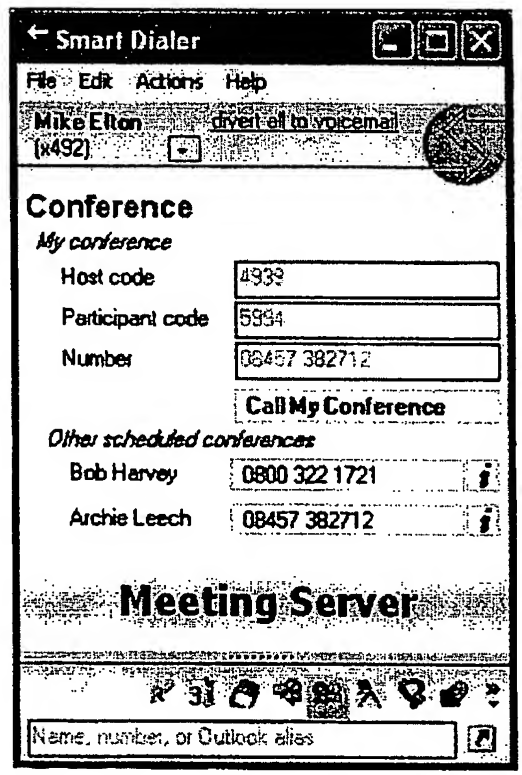
Audio conferencing is now a vital business tool. Where as a few years ago setting up a conference call was a reasonably involved process, these days the majority of conference calls are "reservationless" where users have an access number and a PIN code and they can use this conference call at any time they like.

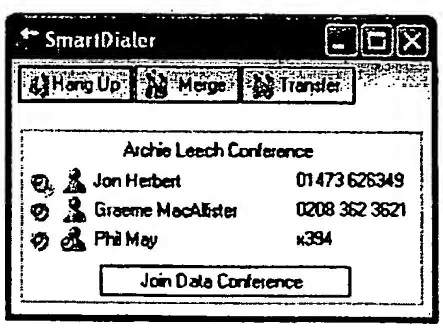
The challenges now for Conference Service Providers (CSPs) are how to

- integrate data conferencing in an easy to use fashion
- streamline the process of signing up new customers
- provide "sticky" content which stops users moving to another provider.

SmartDialer provides an answer to these challenges.

- It allows on-line and automated sign up for a new conference call account.
- Users now have one-click entry into their conference with an in-conference roster.
- When other users of the same CSP invite you to a meeting using their conference call account, these also appear in SmartDialer.
- It integrates with Data Connection's MeetingServer data conferencing product so that data conferencing can be started with a single click.

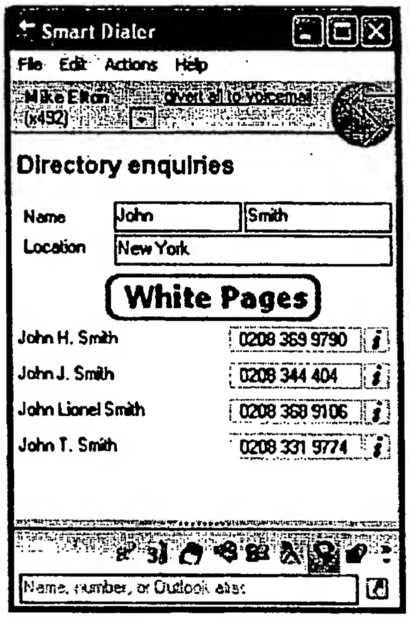


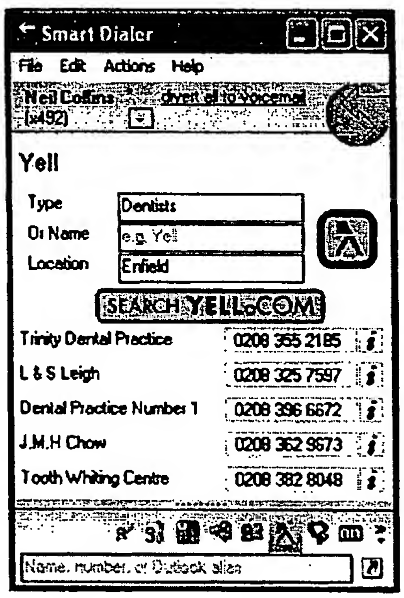


When in the conference, the in call window is extended to show other participants in the conference call.

3.3 Directory Services

Two natural services that lend themselves to the SmartDialer format are White Pages and Yellow Pages, for looking up personal and business telephone numbers.





Through an option on the context menu, it is simple to save a directory contact to the user's office suite address book, and the contact information will persist in the user's Call History.

These services can be provided by the Telco, or by third-party providers.

3.4 DataShare

The Web today is very much a "pull" technology – where users go to web-sites and download what they are interested in. SmartDialer has built into it a new form of web technology called DataShare which allows data and Web pages to be shared interactively between both ends of the phone call.

DataShare requires a DataShare Server to be provided by at least one of the following

- the enterprise of the caller or callee
- the service provider of either the caller or callee.

DataShare works by establishing a shared data connection between two parties. This connection is firewall friendly and can be used to share applications or web pages.

The most common use for this is when a customer phones a company that has a service to offer. Some examples of when DataShare will be used include the following.

- Travel Agent - giving online details of hotels, etc. (see above)
- Cinema booking - offering images and descriptions of current movies, and offering a view of available seats for a showing.
- Sports booking - showing the view from different seating areas.
- Hospitals, Doctors' surgeries, Dentists – showing maps, opening hours, visiting hours, available appointment times.
- Medical Help-lines - advice for common treatments, first aid, maps for medical centres.
- Phone shopping - sharing images of items, shopping basket, current special offers.
- Computer help centres - sharing a client's desktop with the assistant.
- Restaurants – opening hours, daily menus, seating availability.
- Many others - Estate Agents, Local Government information numbers, Post Offices, Hotels, Banks, etc.

Other than the customer-assistant interactions described above, they could also be used for automated services.

- An easier alternative to standard "Press 1 for.... Press 2 for...." phone menus.
- When in a queue a customer could enter their details – speeding up the call process reducing customer waiting times.
- Telephone banking service could offer the capability to enter security information via DataShare, minimising security risks.
- Services that have long queues could provide games, advertisements, special offers via DataShare, to reduce the monotony of waiting.

Once the call is in progress with a business that supports it, a DataShare connection is opened. From that point on, whilst the call lasts, the assistant can choose to offer a DataShare connection. The SmartDial call window will then invite the customer to join the DataShare, giving a short description of the purpose of the DataShare; it will take only one click to open the DataShare connection.

The benefits for the business are also simple. DataShare is a service offered by their Telco, and the DataShare service is easy to integrate (probably with hardware located on site for large companies).

There is also not a requirement for a business to develop entirely new software to support DataShare – for example a theatre/cinema's proprietary booking system can be shared as easily as a website with location information.

3.4.1 Selling DataShare to Businesses

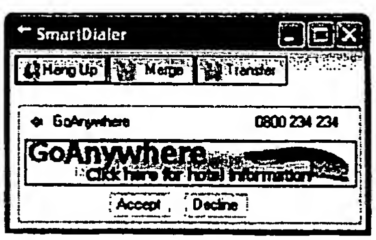
In addition to the client side advantages of DataShare, there is also a revenue stream for Telcos by selling value added services to business which leverage DataShare. This is best illustrated by an example.

PhoneCo is a regional Telco who have already deployed SmartDialer to many home and business users who use it regularly to place calls and pick up voicemail. GoAnyWhere are a customer of PhoneCo and are a travel company with over 100 sales offices around PhoneCo's region.

PhoneCo have provided GoAnyWhere with an innovative business service as follows.

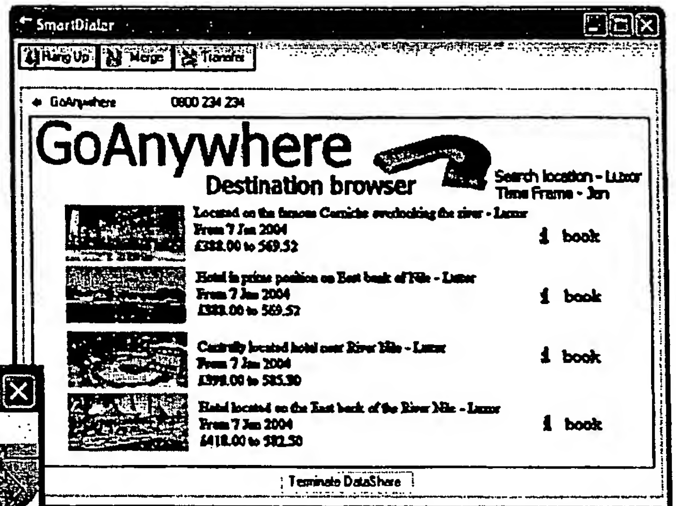
When a user calls GoAnyWhere (perhaps by using the Yellow Pages service of SmartDialer), they go into a phone call as normal.

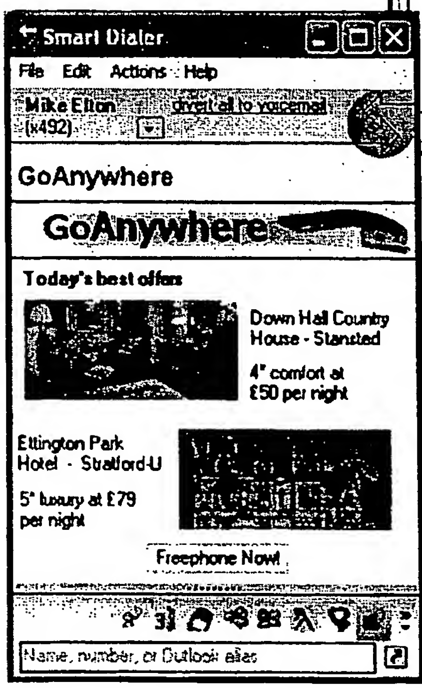
They also see a banner from GoAnyWhere telling them can get online access to hotel information to see the hotels rather than the operator just describing them.



If they press on the button they start a two way data session with the sales representative so they can see images of the hotels they can stay at, etc.

For the sales representative when the call starts they see the "DataShare available" button appear. They then press the button and can share any application on their desktop to the customer. In this case, they choose to share a specially written application which shows the users images of hotels, resorts etc. and can also take booking information.

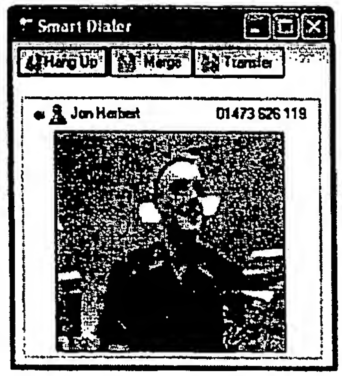




Additionally, users who are regular GoAnyWhere customers can choose to install a "GoAnyWhere" plug-in to their smartdialer.

As well as being a way to do all the above quickly and easily, this plug-in displays information on special offers, personal travel history information for the customer and a link to the special "frequent flyer" scheme which GoAnyWhere manages on behalf of its business customers.

3.5 Video



SmartDialer also supports point to point video calls.

Video calls are setup first by setting up a normal phone call (either by dialling using the phone or using click dial). SmartDialer then uses the following methods to establish a video call (in this order).

- Using point to point SIP and an RTP stream between the two endpoints.
- RTP between the endpoints controlled by a tunneled control connection to a DataShare server.
- Tunneling both the video and control traffic via a DataShare server.

The first of these gives the best performance, the last gives the most reliable connectivity, the middle gives a compromise between the two. So long as at least one of these options works then the users are prompted with two buttons in the call window.

- A "Send Video" button which, when pressed, will send your video image to the other person.
- A "View Video" button which displays the other person's video if they are sending it.

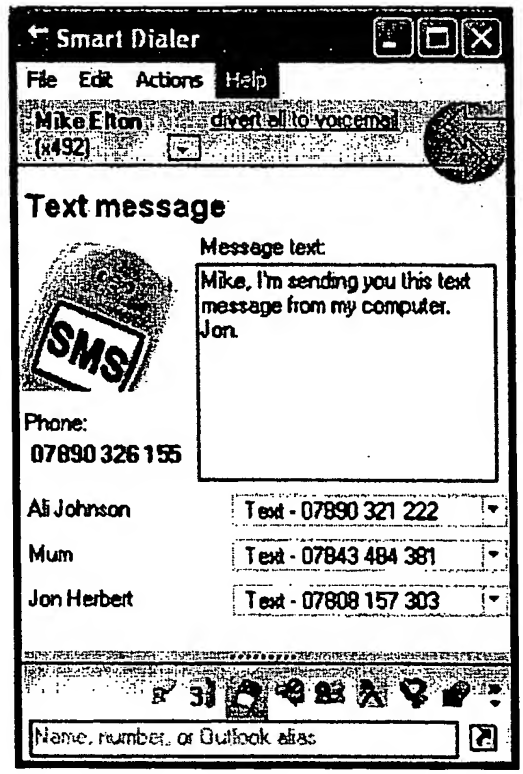
By default (which can be over-ridden) neither button is pressed.

Note that this can also be used to communicate to video enabled mobile devices so long as the Telco has the necessary gateway capabilities.

3.6 Text, Picture and Video Messaging

As a plug-in service for mobile phone users, they can send text, picture and video messages using SmartDialer.

This is specifically targeted at sending to mobile devices but, so long as SmartDialer is allocated a separate phone number (for example as a second line) it can also be used to receive these messages.



SIP MARKET OVERVIEW

An analysis of SIP technology and the state of the SIP market

September 2003

Jonathan Cumming
Director of Marketing, Protocol Software, Data Connection
Jonathan.Cumming@dataconnection.com

Data Connection Limited
100 Church Street
Enfield
EN2 6BQ
United Kingdom
http://www.dataconnection.com

DATA CONNECTION

Executive Summary

Session Initiation Protocol (SIP) is continuing to develop rapidly and it is difficult to keep up with all of its innovations and uses. This white paper is aimed at people who want to understand the concepts and drivers behind SIP adoption, and how it is evolving to face new challenges.

This paper summarizes where SIP has come from, how it works, and what makes it such a useful protocol. It then describes how SIP is used in applications including telephony, conferencing and messaging, and how it is being extended to provide innovative services and accommodate the requirements of real-world deployment, where NATs, service level agreements and regulators exist.

In covering this broad range of SIP-related topics, it provides a summary of the state of this increasingly important protocol.

About the Author

Jonathan Cumming is Director of Marketing, Protocol Software at Data Connection. Previously, he was development manager for DC-SIP, Data Connection's SIP User Agent and Proxy Server Toolkit, and retains product management responsibility for the product.

Jonathan has over 15 years' experience in the communications software industry. He holds an MBA from INSEAD and an Engineering degree from Cambridge University.

Table of Contents

1 Introduction

Session Initiation Protocol (SIP) is a signaling protocol for controlling multi-media sessions. In other words, it provides a way to establish voice, video and messaging communication between devices. From its initial use in Internet Telephony, SIP is spreading into many new areas, including advanced telephony applications, conferencing and instant messaging, and its functionality is expanding to meet the new requirements from its increased scope.

This paper provides an overview of the current state of SIP, and explains both the technology and the business requirements that are driving development in order to give a context in which to understand the issues involved.

This document is not a SIP primer, although it does explain the main concepts and terms that SIP uses, and is aimed at people who are

- working with SIP and wanting to increase their understanding of other ways that it is used
- looking at developing or deploying SIP-capable devices
- just interested in understanding SIP a bit better.

As with any fast-moving field, any document that describes the current state of the market is always out of date, so this paper provides a snapshot from September 2003. Nevertheless, the concepts on which SIP is based and the problems that it addresses do not change, so the majority of this information will remain valid even if the details have altered. The further information section should provide useful pointers for anyone who wishes to investigate particular areas in more detail.

1.1 SIP concepts

SIP's view of the network matches that used in the Internet: intelligent devices communicate directly with each other over a simple transport infrastructure. This contrasts with the traditional telephone network, where transport between dumb endpoints is provided through an intelligent network core that is an active party in any conversation.

This difference allows the network to become a commodity and allows any device attached to the network to provide a service to any other. This increases competition, which drives down prices, and helps innovation, because the investment required to set up a new service is very small. With the traditional intelligent telephony network, only the telephone company can provide new services, and this requires the nctwork core to be upgraded, which is an expensive and slow process.

While the above explains why IP telephony is helping to drive down the general cost of telephony, and why there is a high level of SIP innovation, the following SIP features show why it is such a powerful framework.

- Mobility: SIP allows a client to register dynamically with a fixed location, so that calls can be routed to it using a well-known address, similar to an email address.
- Flexible message structure: SIP's message structure makes it much easier to extend for new applications than equivalent existing protocols, such as H.323 which uses the ITU's opaque ASN.1 encoding standard instead of text, and it is seen as being much simpler and more flexible.
- Distribution of function between devices: SIP enables requests to be dynamically routed through different devices, enabling functionality to be distributed and requests routed through the relevant devices.
- Negotiation of supported features: This makes SIP very adaptable, as the media and protocol extensions to be used for a particular call are negotiated between the clients on that call. As a result, SIP can be used to set up any type of media conversation, including voice, video and messaging.
- Separation of signaling and media: In SIP, the paths of the signaling and the media are totally independent. The signaling and media may traverse different routes through independent sets of devices on different physical networks.
- Forking: This allows multiple devices to be associated with a single address, so that all or a selection of these devices can be contacted simultaneously or sequentially, according to local policy.

These features are equally applicable to many areas, including telephony and messaging, and have been the drivers for SIP's adoption by the major players in these fields.

1.2 Definition of terms

SIP communication is made up of messages that are sent between the devices using UDP, TCP, or another transport protocol. These messages are either requests or responses and contain a set of headers, which are the parameters of the message, and one or more message bodies, as required by the application.

A single SIP request and all its responses form a SIP transaction. Different types of transaction are used for different protocol functions. For example, an INVITE starts a telephone call, and a MESSAGE sends an instant message.

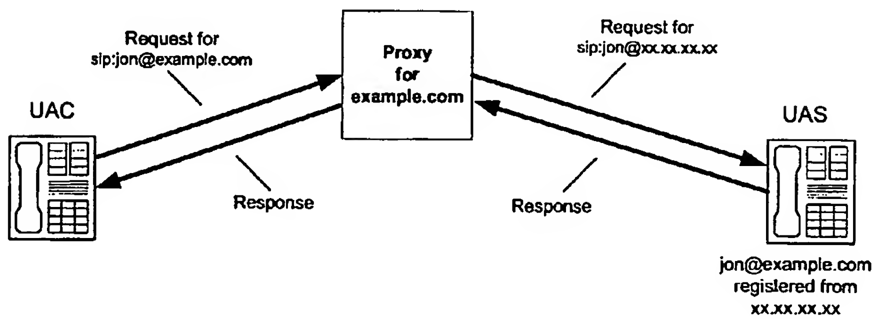
A SIP dialog is a persistent link between two devices that is used to associate transactions and to provide ordering between them. SIP transactions can exist within or outside a SIP dialog, and transactions are used to establish and terminate dialogs. For example, in telephony, the initial INVITE that starts the call also establishes a dialog between the participants. To end the call, one participant sends a BYE within the context of this dialog. This BYE transaction terminates both the call and the associated dialog.

The high-level concept of a call does not simply map to a SIP dialog, because a single telephone call may include conversations with several people and devices, for example receptionists and voicemail systems. These individual connections need separate SIP dialogs, so the call can contain multiple dialogs. SIP messages contain a call identifier field (Call-ID) that is sometimes used to link the dialogs and transaction into an application-level concept of a call, although this use is strictly outside the standard.

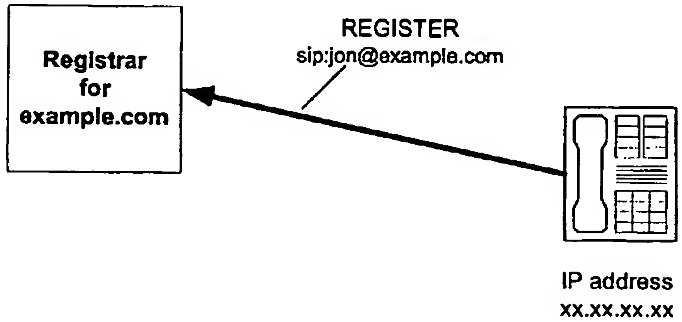
The following terms are used to describe SIP devices.

- **User Agents (UA)** are endpoint devices that terminate the SIP signaling. They can be clients (UAC) that initiate requests, servers (UAS) that respond to requests, or more normally a combination of the two.

- **Proxies** are devices in the signaling path between User Agents that route requests on towards their destination. They may add parameters to the requests and may reject requests, but they may not initiate requests or respond positively to any request that they receive. Proxies pass unrecognized messages through unchanged; this means that many new features can be deployed in a network by upgrading only the User Agents and leaving the proxies to continue with their default behavior.

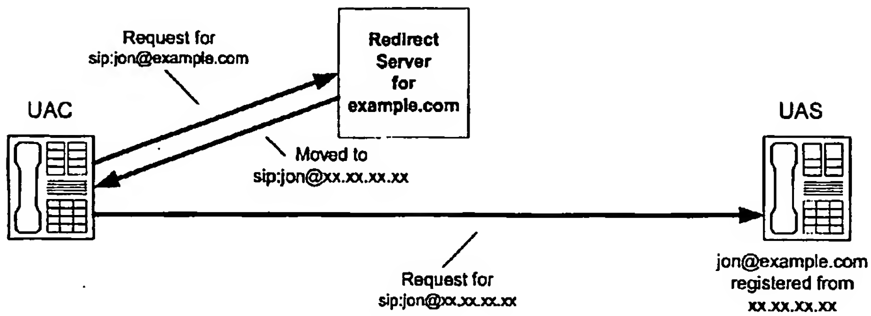


- **Registrars** are specialized User Agent Servers that handle REGISTER requests. SIP devices use REGISTER requests to dynamically register their current location, and this enables them to be contacted when mobile.



The registrar now knows the current IP address at which jon is reachable.

- **Redirect Servers** are specialized User Agent Servers that respond to requests by redirecting them to another device.



The redirect server responds to the request containing the address to which the request should be redirected.

Many real devices contain several of the above elements. For example, a Registrar will normally be linked with a proxy or redirect server, so that the proxy or redirect server can use the location information that it receives to send requests on to the registered devices.

However, the action that a device takes on receipt of a SIP request is not determined purely by the protocol; it is also determined by the application. An application may decide to forward the request on to another server for further processing, such as authentication, instead of forwarding it directly to its destination. The generic term for such a device is an **application server**. From a SIP view, an application server may behave as a User Agent, a Proxy or a combination of the two, depending on the situation.

A common configuration is what is known as a Back-to-Back User Agent (B2BUA) where the device is similar to a proxy in its behavior, but actually terminates the SIP signaling on both sides, so that it can initiate requests to control the dialogs passing through it. This requires that the B2BUA is a trusted party in the communications, which prevents end-to-end encryption and authentication of the messages.

1.3 Where is SIP discussed?

The main forum of SIP standardization is in the Internet Engineering Task Force (IETF), which is the primary standards body for Internet protocols. The IETF has set up the following three working groups to work on the protocol and its application.

- The SIP working group covers enhancements to the core protocol.
- The SIPPING working group covers applications of SIP.
- The SIMPLE working group covers Instant Messaging and Presence applications of SIP.

The distinction between these groups is that the SIPPING and SIMPLE working groups discuss applications of SIP and decide how SIP should be used in each of them. If they determine that the requirements of a particular application cannot be handled by the core protocol, then these requirements are passed to the SIP working group for a solution. This enables the SIP working group to maintain control over extensions to the protocol, while limiting the scope of its discussions.

Other IETF working groups whose areas touch on SIP include the following.

- IPTEL (Internet routing of telephone calls)
- MMUSIC (responsible for Session Descriptor Protocol (SDP), which SIP uses to describe its media sessions)
- MIDCOM (Middlebox communication – firewall and NAT traversal)
- SPIRITS (PSTN – Internet telephony interoperation)
- ENUM (Internet use of traditional PSTN phone numbers)

Several industry groups are also discussing how to standardize the use of SIP in their environment. These include

- Packetcable (www.packetcable.com), who are using SIP for telephony over cable
- 3GPP (www.3gpp.org), who have adopted SIP for 3G mobile
- Multi-service Switching Forum (MSF) (www.msforum.org), which has defined SIP-T conformance levels and is now working to ensure that SIP can be deployed in large scale PSTN networks.
- ETSI TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) (www.etsi.org), who are working to ensure that SIP is suitable for deployable telephony applications.

There is a continual conflict between the requirements of the traditional telephone providers, who need to provide an end-to-end billable solution that meets their regulatory requirements, and the less controlled environment of the Internet. This is resulting in concern over the interoperability of the different flavors of SIP, including 3GPP SIP, PacketCable SIP, and IETF SIP, and discussions are ongoing to ensure that they all work together.

There is a separate initiative to standardize the programming interfaces to SIP and other telephony protocols. This work covers the following interfaces.

- JAIN (java.sun.com/products/jain) – Java APIs to SIP and other Next Generation telecom protocols.
- Parlay (www.parlay.org) – High-level, protocol independent APIs that allow the development of telecommunications applications that are independent of the underlying network.
- Call Processing Language (CPL) - XML-based language that can be used to describe and control Internet telephony services (draft-ietf-iptel-cpl-08).
- Common Gateway Interface (CGI) - HTTP CGI compatible extensions to providing SIP services on a SIP server (RFC 3050)

These standardized interfaces help the development of SIP applications that are not tied to a specific implementation of the protocol. This makes the resulting application more portable and reduces the developer's dependence on one supplier, but they can add a processing overhead that may reduce the overall efficiency of the system. The protocol independent interfaces also limit the ability to exploit the advantages of a particular protocol.

2 History

2.1 The origins of SIP

SIP was originally developed around 1996 in an academic project to control multicast media distribution. Its message structure was based on SMTP (email), with the simple, text-based, extensible form that had helped to make email so successful. When interest in Internet Telephony increased, this initial work was used as the basis of the new protocol, and it was standardized by the IETF in March 1999 as RFC 2543.

SIP has since been extended for use in instant messaging and presence, and continues to find new applications in the establishment of sessions between devices whosc location and capabilities may change.

2.2 How SIP developed

The initial work on SIP received strong backing from the venture capital community, with a number of well-funded companies set up to develop SIP-based products. This, together with adoption by MCI WorldCom, Cisco and ETSI TIPHON, led to an explosion of interest in the protocol.

Early standardization work concentrated on the use of SIP for Telephony (SIP-T), and it became clear that RFC 2543 would have to be extended in many ways to handle all the new requirements. The huge number of extensions that were proposed overwhelmed the SIP working group and led to long delays in their standardization. As a result, the standards lagged behind the requirements, and many new features were added through proprietary mechanisms. Although many of these extensions have now been either adopted as standards or replaced by standard mechanisms, this divergence has led to interoperability problems in function beyond that defined in the core specifications.

After three years of rapid development and extension to SIP's function, RFC 2543 was finally replaced in 2002 by a new set of SIP standards based on RFC 3261. These new standards clarified and extended the original protocol, and improved its scalability and security. Products supporting RFC 3261 are now appearing on the market, although support of some aspects of the protocol, for example transport level security (TLS), is still limited.

In around 2000, 3GPP (Third generation mobile) also selected SIP as the basis for its communications infrastructure, and, as a result, there has recently been a major drive to standardize the extensions required for mobile telephony.

Current work is focusing on areas including NAT traversal, conferencing and security. These and other areas are discussed in more detail in later chapters.

2.3 The return to reality

The initial enthusiasm for SIP coincided with the Internet bubble, as SIP offered a way to replace the existing expensive telephone system. The combination of venture capital backing, which expected short-term returns, and over-optimistic claims from the protocol's exponents placed unrealistic demands on the protocol and the products being developed. This resulted in a drop in the quality of both the standards definition and the products that came to market, as competitors raced to support too many features. In addition, the impression that SIP was a simple protocol resulted in the devclopment of many SIP implementations, written in different programming languages to different versions of the standard, and providing very different levels of quality and completeness. This caused real interoperability problems and raised concerns over SIP's fitness for any commercial purpose.

This "bad press" could have killed the protocol, but with influential backers, including Cisco, Microsoft and Nokia, and its fundamental strengths, SIP continued to develop and mature. Today, there are over 20 SIP-related RFCs and over 100 SIP-related drafts being discussed in the working groups, and almost every major telephony equipment manufacturer is developing SIP-capable products.

Interoperability is improving as the standards and the implementations mature. Traditionally, SIP interoperability has been determined at the closed-door SIPit events that are coordinated by the SIP Forum http://www.sipforum.org. However, although these events are invaluable for ensuring good interoperability, the results are confidential and cannot be used by a potential customer to determine whether particular devices are compatible.

SIP device resellers are therefore assembling product combinations that they have tested to offer complete solutions, but pressure from customers for a better measure of interoperability is encouraging the establishment of independent conformance tests for SIP devices. The first stage in this process is the definition of suitable sets of functionality that should be supported by particular devices. Once these are agreed, it will be possible to establish independent testing of any claims.

Various industry consortia, including the MSF and PacketCable, have developed conformance levels for their applications, and others, including the SIP Forum, are developing a more generic framework for SIP conformance. Many bodies are claiming to produce conformance test tools and programs, but until the standards and conformance levels have stabilized, these will only be able to validate basic functionality.

SIP products are also now being designed to handle real-world requirements of reliability, security and manageability, but SIP is still an immature protocol that has not been proven in large-scale deployments and it is still evolving to support more advanced applications. In normal operation, the protocol is fairly stable and robust, but somc serious issues with the design of the protocol remain to be resolved. For example, there is continuing work to improve the handling of error conditions and the behavior under heavy load. These, and other major issues that must be considered when using SIP in a real environment, are discussed in more detail in Chapter 5.

3 SIP applications

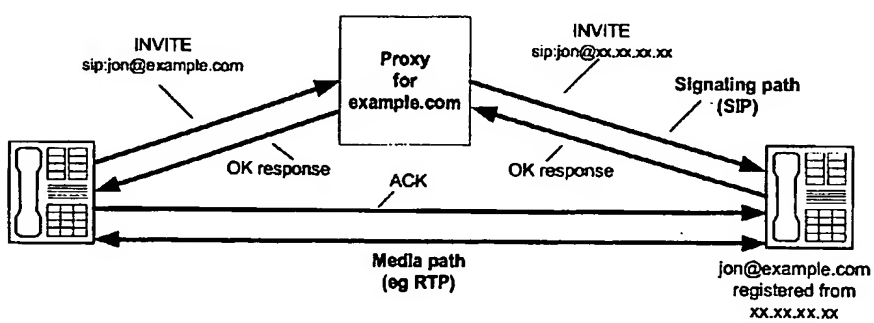
Current SIP use falls into three main categories: telephony (including conferencing), instant messaging and presence. The following sections describe how SIP works in each of these areas.

3.1 Telephony

Protocols for audio and video telephony are, in principle, straightforward in an IP environment, because the underlying network provides a routable infrastructure over which to send the media. However, a usable telephone requires additional features, including the ability to find the subscriber and to negotiate a compatible media type for the conversation.

To make a SIP telephone call, a SIP UA sends an INVITE request. In the message body of this request, it puts the SDP description of its available media channels. This request is forwarded by proxies across the network until it reaches its destination, or until it is rejected with an error response.

When the called UA receives the INVITE request, it checks whether it is capable of accepting the call, and then starts the phone ringing. In the meantime, it sends a provisional response back to the caller to tell it that the phone is now ringing. When the phone is answered, the called UA sends a final positive response with the SDP description of its media channels back to the caller. On receipt of this response, both parties now have the SDP descriptions of the other's media, and can establish the media channels agreed. The caller UA also acknowledges the successful receipt of the response by sending an ACK, which is a special type of request, back to the called UA.



If, during the call, either party wants to change the media, for example to open a video channel, then it can send a re-INVITE (an INVITE within the established dialog) with an SDP body describing the new media. If acceptable, the recipient responds positively with its SDP. Otherwise, it rejects the request and the session continues unchanged. When either party wants to hang-up the call, it sends a BYE request.

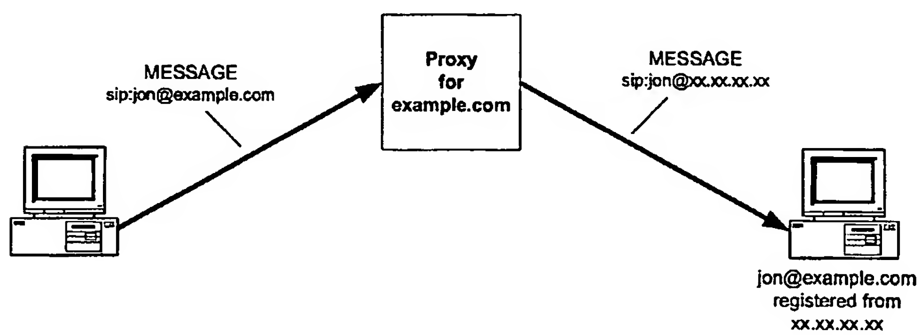
This set of primitives allows the establishment of a telephone service, but there are many complications and variations to this scenario; some of these are covered in Chapters 5 and 6.

3.2 Instant Messaging (IM)

IM provides the ability to send messages to other individuals. The underlying requirement is very similar to email, but the user experience is very different. Instant messages are analogous to the sentences in a conversation; they are normally short, informal, and expect a quick response. Email, on the other hand, is an electronic letter; it has a more formal structure and delivery process.

Many see IM as the next killer application. Existing IM services, as provided by Yahoo!, AOL and Microsoft, have been extremely successful, as has the analogous short message service for mobile phones (particularly in the UK).

SIMPLE (SIP Instant Messaging and Presence Leveraging Extensions) defines how SIP can be used for IM. It uses SIP registration to enable users to be contacted using their URLs, for example sip:jon@myserver.com, at a changing IP address. Messages addressed to the users are then redirected or proxied by their home server onto their current location.



SIMPLE defines the following two modes of operation.

- In page mode, every message is independent of every other. No persistent protocol-level connection is established between the User Agents, and each message is routed independently to its destination. This is directly analogous to the operation of email.

- In session mode, a persistent connection is established between the two User Agents, and a separate media channel carries the message contents. This operates in the same way as in telephony, except that the media session that is established uses Message Session Relay Protocol (MSRP), as defined in draft-ietf-simple-message-session-01, rather than RTP.

The limitation of page mode is that there is no protocol-level link between messages. As a result, although the protocol provides a reliable transport, it lacks flow control and message ordering, and is therefore unsuitable for carrying large amounts of data or high message flow rates.

Page mode also sends all the data through the signaling channel and any routing proxies. This limits the scalability of the solution, because all the messages traverse the central routing proxies. This puts an unnecessary load on what may be a bottleneck, and restricts messages to types that are understood by all the devices in the signaling path.

In session mode, flow control and ordering of the data is provided by MSRP. The data is sent directly between User Agents or through specified message relays. This is normally a quicker route than sending through all the proxies in the signaling path, and it reduces the load on the proxies. For small numbers of messages in a conversation, session mode has a higher overhead because more SIP messages are required and the media channel has to be established and closed. For longer conversations or large amounts of data, session mode is more efficient because the media messages do not need to include the routing and authentication information that would be required in every page mode message.

In some environments, for example financial institutions, additional security or message monitoring is needed, which requires access to all the message contents at some intermediate monitoring device. In page mode, this can be provided in any of the proxies along the signaling path. In session mode, the message relays in the media path can be used instead.

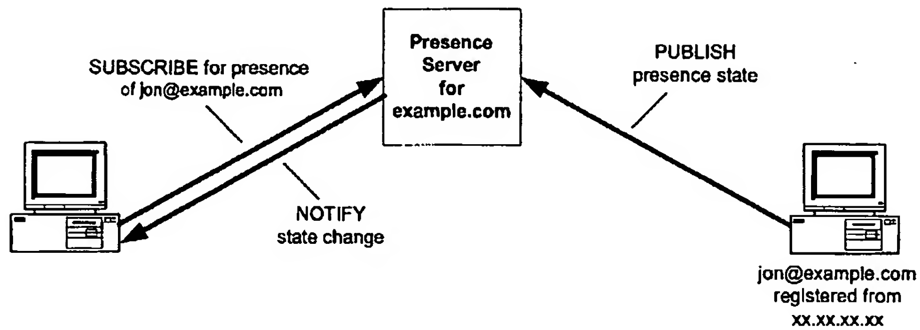
IM is growing very fast, and the use of SIMPLE is growing at an even faster pace, due to the drive towards open standards and the benefits of compatibility between IM and telephony. Current implementations are based on page mode, but the use of session mode will increase, because its improved scalability is required for larger installations.

3.3 Presence

Presence is the ability to publish your state, for example whether you are at your desk, and to subscribe to other people's state and be notified when it changes. For example, this can be used to tell your colleagues whether you are available to take their calls.

Presence is handled in SIP using a generic event monitoring and notification mechanism, which is defined in RFC 3265 – SIP Specific Event Notification. This allows a device to subscribe to an event package that is supported by another device and to receive change notifications from it. Event packages define a set of state information for a specific context; for example, draft-ietf-simple-presence-10 defines the package for presence. Event packages are being defined for a wide range of applications.

Presence also defines the concept of a presence server. A presence server collects the presence state from a set of devices, and enables a client to subscribe to it in order to receive notifications whenever the state of these devices changes. The advantage of a presence server is that an individual device only has to publish its state to a single server, rather than to each interested party, which aids scalability.



Presence is normally used with telephony or IM, and it is this combination that is so powerful. For example, an intelligent proxy can automatically route calls directly to your mobile phone when you are out of the office, or a conference server can start a conference and invite a pre-arranged set of participants as soon as all the key people signal their availability. However, the most common use of presence today is between friends and colleagues.

The use of presence in an informal environment works well, but there are privacy concerns when it is used more widely. In particular, who should be told what information about you, what is a suitable level of detail, and what are they allowed to do with this information? There are some very subtle effects of this; for example, will you appear rude or inefficient if you ignore a phone call after having published your availability? As a result of the increased information that is available about us, we are going to have to be much clearer about what information we want to give to whom, and how it might be used to monitor us. This issue is not completely solved, and it is discussed in detail later in section 5.6 on Privacy.

Finally, it is not clear how the increased information that presence provides will affect productivity; given that interruptions generally lower one's efficiency, and the existence of presence information is likely to increase someone's likelihood of contacting you, will the increased number of interruptions lower productivity, or will the time saved from only calling people when they are available and the increased responsiveness raise it?

Presence is an extremely powerful feature, as the earlier examples demonstrate, but it will be the societal issues that will limit its acceptance of presence, rather than any technical ones.

4 SIP deployments

SIP can be used throughout a network: as a peer-to-peer protocol between endpoints, between the endpoints and the devices in the core, and between devices within the core. However, SIP can also be used only in parts of the network. The reduced scope of this sort of limited application makes it suitable for early adoption of the protocol, because it requires only a subset of function and interoperability with a limited range of devices. Today, SIP is being used in a range of situations: as an end-to-end protocol by early adopters, and as part of the telephone network to back-haul traffic over IP links between switches. It is therefore forming an ever-larger part of the network as the protocol matures.

The initial driver for SIP adoption in telephony was cost, but as the monopoly of telephony service providers has been reduced, prices have dropped in many markets to a level where cost is no longer a significant factor. For example in Japan, Yahoo!BB has been so successful at attracting customers to its SIP-based telephone services that NTT, the incumbent supplier, has been forced to respond with similar pricing plans.

In the future, SIP adoption will not be driven primarily by cost, but by the new services that it can provide and the convenience of converged voice and data networks.

4.1 Existing SIP services

Current SIP use falls into the following categories.

- Internet-only services. These consumer-orientated services provide a central SIP registrar and enable free calls across the Internet to other SIP phones. There may also be some interconnectivity with the PSTN, but only to freephone numbers and with limited ability to receive calls, because in both cases the party on the PSTN side pays for the call. No charges are levied and therefore minimal security and administrative overheads are required. The Internet provides the bandwidth for the SIP signaling and media.

  Free operators, including Free World Dialup, are offering this type of service as a loss-leader, in order to establish a strong market presence that they hope to be able to exploit in the future. There are strong precedents for this business approach on the Internet in the form of Google and Hotmail.

- PSTN and Internet service. In addition to calls between SIP phones across the Internet, the service provider supplies PSTN gateways to allow calls to be made to PSTN numbers, and a phone number that allows calls to be made directly to the SIP phone from the PSTN. This requires a commercial arrangement between the user and the service provider, and Vonage, Deltathree and MCI (WorldCom) all provide this type of service. The overhead of maintaining this commercial relationship makes this commercially viable only for high volume users. However, where there is existing commercial relationship, for example with a DSL service provider, telephony offers a very easy add-on; this is the model being used so successfully by Yahoo!BB.

- Enterprise use. In this case, the service is provided within an organization for inter-office calls, and through gateways controlled by the enterprise into the PSTN. There is only a single commercial relationship between the enterprise and the telephone company, so this offers an efficient way to make a large cost saving.

- Specialized Use. SIP can also be used to back-haul traffic between particular switches, or to communicate between components within a single system. In these situations, SIP is only being used internally, so the business case is purely based on its effectiveness for the purpose against any competing technologies.

As Internet telephony becomes more popular, these models are likely to evolve into a structure that offers end-to-end SIP between what are currently islands of SIP, with the increased flexibility and functionality that this offers.

Practical deployment issues and governments regulations, including QoS, wire-tapping and access to emergency services, may restrict this spread, and these issues are discussed in the following chapters. In addition, the incumbent telephony service providers will attempt to restrict the growth of SIP telephony through regulatory pressures and predatory pricing.

4.2 Interoperating with other protocols

SIP is only one of many protocols being used to provide telephony and messaging services. There is therefore demand from customers to provide services between these protocols, and a number of manufacturers are developing gateways to do this conversion. Interoperability of basic function is normally straightforward, and the complexities arise when mapping more subtle concepts between the systems: for example state levels when the scales do not match, or permissions when the same group concepts do not exist.

There has been a great deal of work on interoperability in telephony in the various standards bodies to produce standard mappings. These include RFC 3398, which defines the mapping between ISUP and SIP messages to provide ISDN/SIP interoperation, and draft-ietf-sipping-qsig2sip-02, which proposes a mapping between Q.SIG and SIP.

In IM, although the major providers have agreed to standardize on SIP, and many of their proprietary protocols are being phased out, the IETF is standardizing two IM protocols: SIMPLE, which is SIP-based, and Jabber, which is an XML-based standard from the open-source community. Both protocols provide similar functionality and will have to co-exist, and there are proposals to use SIP to establish Jabber sessions.

Standardization of protocol conversion is incomplete and some aspects will always remain proprietary, but significant work has been done to ensure interoperability across a heterogeneous network. This work will continue, driven by the need for SIP to be installed into existing environments and to interoperate with a huge range of existing devices.

5 Issues complicating SIP deployment

Chapter 3 described how SIP can be used to provide simple telephony, IM and presence services. However, commercially deployable technologies require a far richer feature set, and the following sections cover some of the issues that need to be addressed in real products.

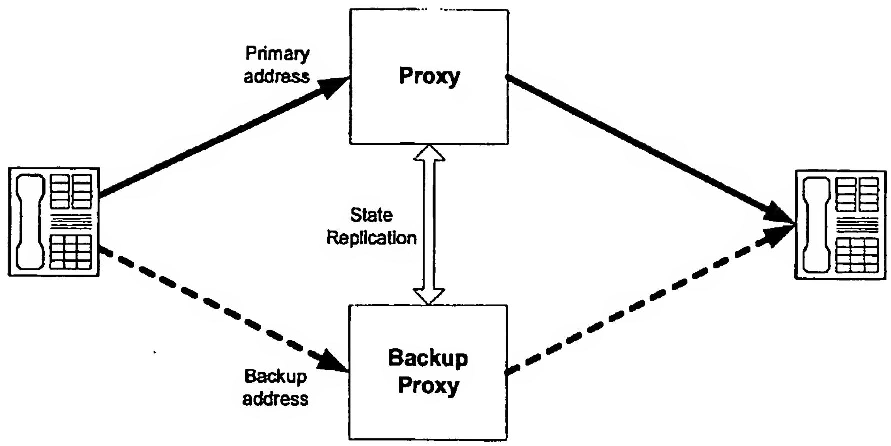
Although SIP standard solutions now exist for many of these areas, the required features are still missing from the current generation of SIP devices because this functionality has only recently been standardized. Therefore, the solutions described may not yet be deployable.

5.1 Reliability

Telephone services are expected to provide a very high level of reliability. This is often referred to as "5 9s" and indicates that the service should be available 99.999% of the time, or less than 5 minutes' downtime in any year, including system maintenance and upgrades. Mobile telephony and IM have traditionally had a lower level of reliability, but expectations even in these areas are rising as the technologies mature. Traditional PSTN equipment provides this level of reliability using expensive fault-tolerant hardware, but SIP attempts to provide it using Domain Name Service (DNS) to reroute the messages around failures.

DNS provides the mapping between services, domain names and IP addresses, and it allows multiple alternate domain names to be configured for a single service and multiple IP addresses to be configured for a single domain name. Using DNS, a SIP device can retrieve the list of alternate addresses and, if its request to the first one fails, it can automatically reroute the request to an alternate backup address.

Using DNS, it is possible to remove any single point of failure from the system, but this does require state replication between any stateful devices in the system. These will normally include any User Agents clients and any proxies that are controlling the allocation of resources.



However, for a SIP device to reroute a message requires it to detect that the initial request has failed, before attempting to use an alternative address. When using SIP, this detection mechanism may be very slow, particularly over UDP. In addition, each new request should also be routed using the same algorithm, so it too will be routed first to the failed server and will exhibit the same poor recovery characteristics. The issues raised by this are discussed in more detail in <draft-sparks-sip-noninvite-00>.

The use of a reliable transport protocol such as TCP or TLS, instead of UDP, greatly improves the speed of failure detection, but this relies on the failure to establish a reliable connection, which also takes time to detect. Proprietary mechanisms that continually monitor the status of partners are required for more responsive recovery. The use of such mechanisms is pushing the architecture towards that used in the traditional telephony network, where the transport layer continuously monitors the state of the links between a defined set of connected switches.

Alternative solutions use redundant hardware to provide failover within a single box, or in a cluster. These techniques enable the remote party to be reasonably unaware of a failover: any TCP or TLS connection and any outstanding transactions may fail, but existing SIP dialogs should continue unchanged. One complexity in these solutions is that the IP addresses must remain unchanged during any failover; this can be achieved using a load-balancing front end, a redundant LAN routing protocol, or by the backup taking over the real IP address of the failed machine.

5.2 Security

The requirement of any security framework is to enable the identification of participants, and to ensure the integrity and confidentiality of any conversations. SIP was not originally designed to be secure, as it was developed to operate within reasonably trusted environments. This makes the protocol more efficient when used within a trusted world, but, as a result, it is vulnerable to attacks from

- external devices
- devices in the signaling path (man-in-the-middle attacks)
- endpoints.

Example of attacks include

- espionage, including eavesdropping and monitoring to obtain private information
- fraud, to gain unauthorized access to resources or to avoid payment
- denial of service (DoS) attacks
- use of incorrectly formed messages to exploit flaws in specific devices.

These security issues, which are described in detail in RFC 3261, are being addressed by extensions to the protocol, including the following.

- The sips: prefix, defined in RFC 3261, which is analogous to https: and mandates the use of a secure transport protocol, such as TLS, between trusted entities. This limits the ability for external devices to launch successful attacks.

- S/MIME (RFC 1847) support for end-to-end message authentication and validation, and encryption of message bodies. These protect from man-in-the-middle attacks, as they prevent intermediaries from accessing or modifying messages.

- Enhancements for Authenticated Identity Management in SIP <draft-ietf-sip-identity-01>, which proposes a mechanism for validating that the author of a message is reachable using the return address given.

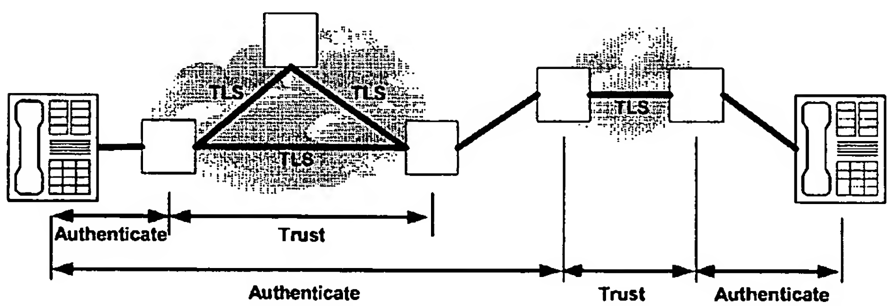
- SIP Authenticated Body (AIB) Format <draft-ietf-sip-authid-body-02>, which provides a portable message signature to verify the author of a message.

However until these extensions are widely deployed, SIP networks will remain vulnerable.

These mechanisms provide the ability to authenticate the participants and secure the SIP communications, but it is unlikely that the entire network will use a single point of authentication. As a result, the security architecture is likely to include

- a shared-secret based authentication to identify endpoints to a local server using a username and password
- established trust relationships between servers with key-based authentication and secure transport
- identity authentication provided by the local server, on behalf of the endpoint, for other endpoints that need to validate the endpoint's identity.

This model can be extended with separate secured network segments, with trusted relationships internally and authentication at the borders.



In the above example, authentication at the border of each domain is made directly with the calling UA. However, an individual user may not want to negotiate separate agreements with every network provider, so agreements will often be made between providers to allow seamless transition over their combined network.

SIP provides an extensible authentication architecture that enables it to use a variety of authentication algorithms. SIP extensions for each algorithm define how SIP carries the particular fields required by that algorithm. The draft <sip-ietf-sipping-aaa-req-03> describes the Authentication, Authorization and Accounting requirements for SIP in more detail. In many systems, the authentication itself may be delegated to a separate authentication server that holds the authentication policies and keys. This can use a protocol such as RADIUS.

5.3 Quality of Service (QoS) and Resource Reservation

When making a telephone call, it is expected (and regulated) that

- the delay before it is possible to speak after the call is connected will be short
- the sound will be reasonable (low jitter and packet loss)
- the delay across the network (latency) will be acceptable
- the call will not be charged for unless it succeeds.

This requires mechanisms to

- guarantee media availability when a call connects and before billing
- control the bandwidth and latency of the media.

The base SIP standard contains no mechanisms for controlling network bandwidth and latency availability, and most current IP networks do not provide this either. However, with the rise of MPLS-based networks, and the use of SIP to control media flows over ATM and other QoS networks, guaranteed quality can be provided.

The use of SIP over non-IP media networks is supported through extensions to SDP to sct up the non-IP media channels. For example, RFC 3108, Conventions for the use of the SDP for ATM Bearer Connections, defines how to use SDP to negotiate ATM channels. QoS is provided by the underlying network and negotiated end-to-end using these parameters.

On an IP network, there are two main ways in which a service provider can provide guaranteed QoS across its network. These can be characterized as follows.

- Integrated Services (IntServ) networks use a protocol like RSVP (RFC 2210) to set up a separate bandwidth reservation across the network for each requested media stream. This process reserves resources on every link and at every node that the media path traverses. The problem with IntServ is that it does not scale, because every media reservation requires explicit bandwidth allocations at multiple devices. This generates a huge volume of traffic, especially for VoIP, where a large number of calls are either very short or never get answered. IntServ is therefore not suitable for large VoIP installations.

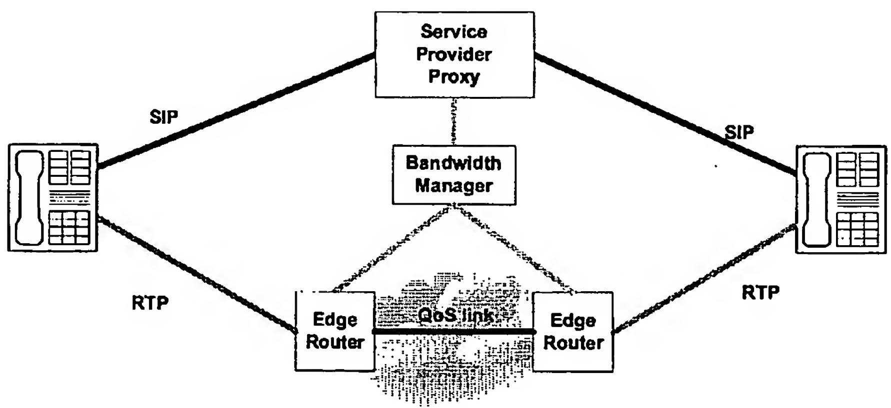
- Differentiated Services (DiffServ) networks classify all traffic into a series of predefined classes, and then prioritize this traffic throughout the network based on its class. This requires DiffServ-capable routers throughout the network to understand the prioritization and to modify their behavior accordingly, but does not require separate reservations for each media stream, so this mechanism does scale.

DiffServ networks also require routers at the boundaries of the network to assign priority to packets received from the outside, and to monitor the traffic to ensure that the network is not overloaded.

Whichever mechanism is used, the service provider needs to control access to the network so as to ensure that adequate resources are available to meet the agreed QoS levels and to prevent degradation of the network by unauthorized traffic. This control will normally be provided by a device at the edge of the network, an Edge Router.

To use SIP across such a QoS network requires a SIP proxy in the signaling path to understand any media requests and open the necessary pinholes in the Edge Router firewalls. This works as follows.

- When the SIP request reaches the proxy, the UA and proxy negotiate the parameters required for the media path. The proxy instructs a Bandwidth Manager to set up the media channel.
- The Bandwidth Manager is responsible for authorizing media channel requests made by through the Service Provider's SIP Proxy. It monitors the loading on the network and controls the Edge Routers' policy to ensure that QoS is maintained within the network. It will open and close pinholes in the Edge Routers to let specific media channels through the network in response to requests from the proxy.
- When the Edge Router receives the media, the necessary pinholes have already been opened, so the media can pass through the network with a known QoS.



It would be possible to use a SIP B2BUA at the boundary of the provider network, and to hide the reservation process from the UA. However this would limit the new services that the UA could develop, because the B2BUAs in the network would have to understand any extensions in order to be able to allocation the right resources. Involving the UA in the reservation minimizes the intelligence that must be implemented in the network core.

RFC 3312, Integration of Resource Management and SIP, defines an extension to SIP that enables media reservation before the phone rings. This ensures that, when the phone is picked up, the media channel is already in place. RFC 3313, Private SIP Extensions for Media Authorization, defines how this can be used to negotiate and reserve the quality of the media channel, and to refuse the call if a suitable channel is unavailable. This feature is not yet widely available, but is increasingly being mandated for equipment in the core of the network.

Currently, QoS is not normally provided out into a customer's LAN, but when voice and data start sharing the same LAN, QoS becomes important. This is because voice requires a fairly low bandwidth to be available on demand with consistent latency to provide good sound quality, but it is fairly tolerant to transmission errors. On the other hand, data can use high bandwidth and can handle high and variable latency, but is intolerant to errors. If these two very different types of traffic are mixed on the same network without differentiation, the overall performance will degrade rapidly as the loading increases. When QoS does become available in LANs, support for RFC 3312 and RFC 3313 will also be required in SIP phones to provide end-to-end QoS.

5.4 Scalability

The existing PSTN network supports billions of telephone subscribers; this is a huge number of addresses to track and for which to maintain routing information. The network also has to handle large numbers of calls, particularly at peak times, with consistent reliability. This presents two separate scalability issues: the first is the ability to route quickly to the required destination during call set-up, and the second is the ability for devices in the core of the network to handle the traffic associated with all the active calls.

For call setup, SIP uses the proven, scalable DNS framework as described above. DNS can handle the required number of addresses and is able to control local caching, which allows consistent information to be distributed throughout the network and minimizes the load on the master database. SIP proxies spread through the network can then provide distributed SIP routing and authentication. Once a call has been established, SIP provides direct communication between the devices over the IP backbone, without any centralized point of control that might become a bottleneck.

Within an individual server, the SIP protocol also scales well, because it includes identification fields for rapid matching of messages to dialogs and transactions, and suitable implementations can load balance across clusters of machines using DNS.

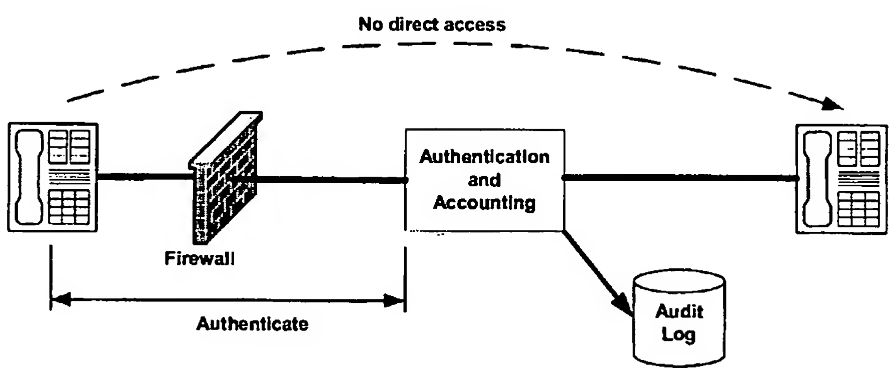
However, because of security, audit and network incompatibilities, both the signaling (SIP) and the media (RTP or another protocol) are often routed through intermediate devices that do more processing than just IP forwarding. One example is recording for billing or an audit trail, where a company, service provider, or government diverts all traffic through a specific device to record the required information. In such situations, these intermediate devices are in the path of all the communications and may become bottlenecks for the machines that they serve.

QoS also imposes a heavy load, as it requires the monitoring of bandwidth usage and availability through the network. IntServ does not scale well, because it requires a separate bandwidth reservation across the network for every call. DiffServ or MPLS-TE based solutions scale better, because the bandwidth allocation is performed at a higher, aggregate level, but these require a second level of control and monitoring to ensure that the allocated resources are not themselves overloaded.

5.5 Accounting

In order to charge for something, it must be possible to monitor and control access to it. This requires the ability to identify users (authentication), check that they are eligible to use the resource and then permit use (authorization), and record the usage (accounting). Authentication and checking of eligibility using SIP is covered in section 5.2, Security, above, and control of access and monitoring are covered in this section.

For services that are accessed through the signaling, for example status requests using SIP Events, proxies on the signaling path can control and monitor usage, although it must not be possible to bypass the accounting proxies to access the resource directly. This can be achieved using TLS or a firewall to limit direct access to the resource.



For media-based services, like telephony, the network must be able to restrict access to the media; this is only possible in a network that limits direct communication between endpoints. Billing records can then be linked to the resource reservations, as described in Quality of Service (QoS) and Resource Reservation above.

A non-QoS network can use firewalls to control media access in a similar way. These can be managed using the same techniques, with the firewall opening media pinholes and tracking usage. However, an extremely strict firewall policy is needed to prevent a customer bypassing the firewall, and such control limits the general usability of the network, although this solution may be suitable for dedicated telephone networks.

More generally, SIP signaling is not designed for the time-based billing used in traditional telephone networks. The separation between signaling and media that SIP provides makes it difficult to time calls accurately, as is required by telephony regulations. This is an area of ongoing study and debate.

A prepaid service, where the network retains the ability to disconnect a call after it has started, imposes further constraints. In the earlier examples, the intermediate gateways authenticate the user and participate in the media negotiation, but otherwise stay in the signaling path only to handle media changes and to clean up at the end of the call. In SIP terms, the gateways are proxies, because they cannot initiate requests. However, the prepayment application server retains control of the call signaling, and is therefore a B2BUA rather than a proxy. This distinction is important when deciding how to design a SIP server to provide a chosen set of services.

5.6 Privacy

Privacy is the control of information, including

- who receives what information
- the level of detail that is provided
- what the recipient is allowed to do with any information received.

This is a complex area to define and even more difficult to enforce. For this reason, government regulations exist to control the behavior of some recipients of private information.

Using SIP, private information may be distributed through the following two mechanisms.

- Implicit distribution. Some information is required for the protocol to work. This includes headers to tell the recipient who has sent the message and how to reply, as well as lower level information, such as the IP address to which the media must be sent. SIP UAs can avoid much of this information by obscuring the return addresses and many other identifiable fields, but they are unable to remove all indications of the message source. In order to provide a fully anonymous service, a separate anonymizing server (implemented as a B2BUA) is required in the signaling and media paths to hide all identifiable fields.

- Explicit distribution. The UA may choose to provide information to trusted third parties, however it may want this to be hidden from others. For example, a network may require user identification for authentication purposes, which should not be passed to the destination. In these cases, the recipient of the information must remove it from any messages that are passed on and must restrict its own use of the information.

  For presence information, this situation is even more sensitive, as a much richer set of private information is being made available to third parties. This requires the ability to specify which groups of users can access each part of its state information.

RFC 3323 describes the requirements for maintaining privacy in more detail, and how privacy servers within the core of the network can provide this. Work on maintaining privacy of presence information is ongoing.

5.7 NAT and Firewall traversal

NATs (Network Address Translators) exist to overcome the limit on the number of available IPv4 addresses, and to provide privacy and security for devices within a private LAN. All NATs set up bindings between external IP address/port combinations and internal IP addresses and ports, to allow packets to be routed back from the external network to devices within the LAN that do not have a globally routable IP address. These bindings may be statically configured to allow access to services within the LAN for external users, for example a website, or dynamically configured to allow packets to be routed back to an internal machine for a particular communication session.

Firewalls implement an organization's security policy and may be configured to allow or disallow particular protocols, including SIP. They work by restricting the flow of packets through them based on configurable criteria, which may include the packet's source or destination address or port, or the protocol being used. It is the responsibility of the organization to configure its firewall to allow or disallow SIP traffic according to its own policies.

NATs and firewalls are often co-resident, because the management of NAT bindings is readily integrated with additional security. However, they are logically separate in their function, and it is only the NAT function that presents a technical challenge for SIP to overcome; it is not the intent of SIP to bypass firewall policy, though SIP should be firewall-friendly.

5.7.1 Types of NAT

There are different types of NAT, distinguished by the characteristics of their bindings. The following lists the major types of NAT.

- Basic NATs do not change the port number. The bindings link an internal IP address to an external IP address for selected ports, but the port numbers are unchanged across the NAT.
- Full-cone NATs set up a single binding between an external IP address and port, and an internal IP address and port. Once this binding is established, any packet that is received from the external network to this address and port will be forwarded to the internal address and port.
- Restricted cone NATs (and Port restricted cone NATs) operate as above, but only accept packets that are received from the same IP address (IP address and port) as the destination of the outgoing packet that established the mapping.
- In each of the above cases, a particular internal IP address and port always maps to the same external IP address and port. However, Symmetric NATs set up a different binding each time, so the same internal IP address and port may appear as different IP addresses and ports to different destinations, and several devices can share the same external address and port when communicating to different remote hosts.

These NAT characteristics result in the following effects.

- The party inside the NAT must initiate communication to each remote address and port to create the new dynamic binding, or a separate protocol must be used to create new bindings. If no external mechanism is used to create the bindings, then a device behind a NAT may be able to make SIP calls but not be able to receive them. Even in this situation, symmetric RTP must be used to allow media to flow in both directions through a single RTP connection initiated from inside the NAT.

- To maintain a dynamic binding, packets must be sent between the partics at regular intervals (the required frequency of these retransmissions is not defined and can be under a minute), or the communication must use a session-based transport, such as TCP. For this reason, the use of a session-based transport protocol is strongly recommended. If UDP is used, then the device behind the NAT must continually resend registration or other messages to maintain the bindings, which is a waste of resources.

- Two ports on the same internal address may be mapped to different external IP addresses, and the external ports may bear no relation to the internal ports - as a result, the value of addresses and ports cannot be inferred from the other addresses or ports. This breaks some of the existing standards that assume a numerical relationship between port numbers. Several extensions have been developed to address this issue, including RFC 3581 for symmetric response routing in SIP, and draft-ietf-mmusic-sdp4nat-05, which extends SDP to specify additional port numbers for RTP.

- An internal device has to use a separate protocol to determine the address at which it will appear to external devices. In SIP, this requirement is minimized because the recipient of a message sets the return address to be the address from which the message is received, rather than address that the sender believes is correct. However, additional protocols are required to determine valid addresses for the media.

These issues are common to all VoIP protocols, not only SIP, so the IETF has established the MIDCOM working group to discuss general solutions to NAT traversal by VoIP. Their solutions fall into the following categories.

- NAT detection protocols that allow a device inside the NAT to determine the NAT's behavior and bindings indirectly, and to modify the protocol messages appropriately. STUN, as defined in RFC 3489, describes such a protocol.

- NAT control protocols that allow a device inside the NAT to control the NAT to set up dynamic NAT bindings and to determine the external address that will be presented. uPnP provides one mechanism, which is supported by Microsoft and is being discussed by the uPnP forum, rather than the IETF.

- Application Level Gateways (ALGs), which modify the signaling messages and may provide a media relay. ALGs can work around limitations in the protocol and provide a short-term solution. These are discussed in more detail later.

- Relays in the external network with globally routable addresses to relay the messages. TURN provides this functionality.

NATs are not required in IPv6 networks, so it is hoped that they will eventually disappear, but they will exist for many years, and SIP must work through them.

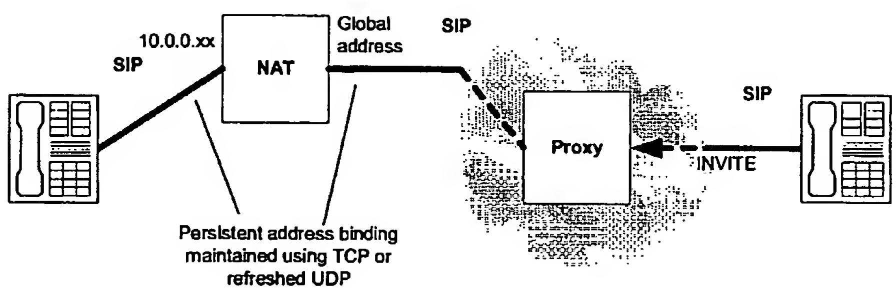
This functionality is likely to change as the standards for NAT and firewall control improve, and the best solution will be a combination of the above, dependent on the precise scenario.

5.7.2 Using SIP through NATs

As mentioned earlier, SIP contains several features to help its operation through NATs, but the following issues still remain.

- How do you send a SIP message to a device that is behind a NAT?
- How do you establish a media session with it?

Once a device has received a SIP message from another device that is behind a NAT, it can respond to the address and port from which the message was received, and these addresses remain valid as long as the NAT binding is kept alive. However, if the first SIP message is to the device behind the NAT, another mechanism is required. This first SIP message can be sent through the proxy with which the device registered its location, as long as the device maintains its NAT binding with the proxy. As discussed earlier, this can be achieved by using a TCP connection or by refreshing its registration at regular intervals. By Record-Routing all requests, the proxy can also ensure that it remains in the path of all future requests, and that external devices do not try to contact the device behind the NAT directly. As result, this mechanism works for even the most restrictive NATs.

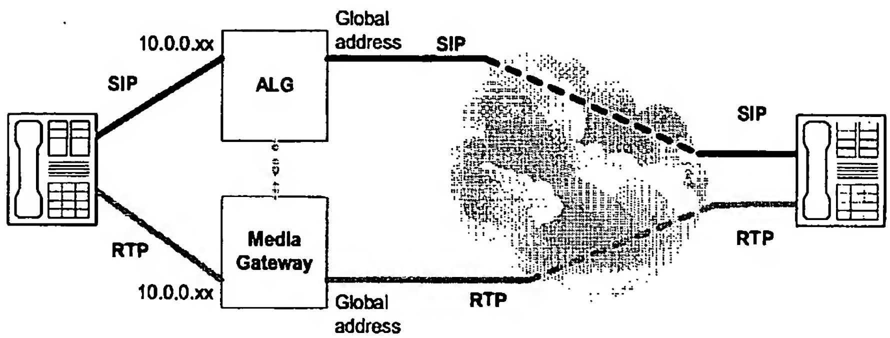


When only one device is behind a NAT, the device behind the NAT can successfully start the media session and, by using symmetric RTP, this session can be used to send media in both directions. However, when both devices are behind NATs, the situation is more difficult because neither has a valid address with which to establish the media session. If another protocol is not available to determine a globally routable address to which to direct the media, then a media relay may also be required.

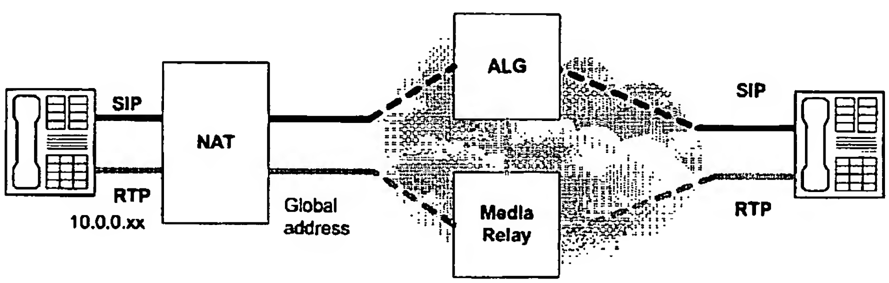
5.7.3 Application Level Gateways (ALGs)

ALGs are devices that understand higher-level protocols, and may dynamically open additional pinholes through the firewall to let data through according to each protocol's requirements. For example, a SIP ALG may open pinholes in the firewall to allow the media to flow.

ALGs can also be integrated with NATs and be used to modify the messages as they pass through to convert any internal IP addresses to their external equivalents. This provides a method for NAT traversal that does not require any changes to the endpoints.



An ALG can be positioned outside the NAT to enable SIP communication with devices behind a NAT. In this situation, it incorporates a media relay and modifies the SIP messages to direct all media through its relay. Because the ALG presents globally routable addresses, it can successfully set up connections with endpoints that are behind a NAT, and can therefore be used as an intermediary in calls between endpoints even if both are behind NATs.



Because of their ability to work through NATs with the current generation of SIP, ALGs are a fundamental part of today's SIP offerings and form the basis of specialized products such as Session Border Controllers. However, SIP ALGs are implemented as B2BUAs, not proxies, because they modify the SIP signaling messages beyond that allowed by a proxy. As a result, there are various problems with ALGs, including the following.

- The SIP messages cannot be encrypted end-to-end, because the ALG needs to be able to interpret it. This limits security and privacy and makes the ALG a trusted party in all communication.
- The protocol cannot be extended without upgrading the ALG. Again, the ALG needs to understand the protocol to control the firewall or media relay appropriately.

For these reasons, ALGs are not able to support new protocol extensions and servicc innovation by end users, and cannot be recommended as a long-term solution.

5.7.4 Devices behind the same NAT

If both of the endpoints are behind the same NAT, it is more efficient for them to use the internal IP addresses instead of globally routable addresses, because the messages can then remain within the LAN. For both SIP and SDP signaling, this can be achieved by using a fully qualified domain name rather than an IP address to advertise the server ports, and by providing a local DNS server that returns the internal address rather than the globally routable IP address. However, if a globally routable DNS address for the endpoint does not exist, this solution is not possible. Also, not all endpoints may support domain names within SDP, which limits the applicability of this solution in some environments.

A fuller explanation of the scenarios and a mechanism that handles many of these scenarios is presented in <draft-rosenberg-sipping-ice-01>.

5.8 Device configuration

SIP devices do not require a lot of configuration information, but the way that this information is entered varies significantly between devices. This makes support of SIP devices more complex than it should be.

The following configuration information is normally required.

- Local (outbound) proxy, to handle local policy and NAT/firewall traversal
- Registrar (one or more)
- Username and password (one or more)

Rather than agreeing a single standard mechanism for automated configuration under centralized control, several alternative mechanisms are being recommended. These include the use of RFC 3361 – DHCP Option for SIP and well-known DNS and multicast addresses. To coordinate these separate mechanisms, draft-ietf-sipping-config-framework-00 defines a single configuration process that tries each in turn until one succeeds.

In some environments, it is unclear who should control the endpoint configuration. For example, users may need different outbound proxies depending on the service required and may not want their network service provider to control this choice, whereas the network service provider may have a financial incentive to route all of the SIP traffic through its servers. In others environments, for example enterprises, centralized management can be used to minimize end-user support and enforce corporate policy. Different solutions may therefore suit each situation.

Endpoint configuration is also possible using SNMP, or another MIB-based management protocol. The standard MIBs for the configuration and monitoring of SIP devices are well advanced <draft-ietf-sip-mib-07>, although arguments remain over the level of detail that should be available through the MIB. MIBs are particularly suitable for the management of larger SIP devices, such as servers, where they provide a high level of configuration detail and status information and can be easily integrated into a larger system management suite.

5.9 IPv6

The introduction of IPv6 is being driven by the lack of IPv4 addresses, particularly in the Far East, by the standardization on IPv6 for 3G mobile, and by government initiatives in countries including the UK and US.

SIP and SDP are fully compatible with IPv6, so are ideally suited to this environment.

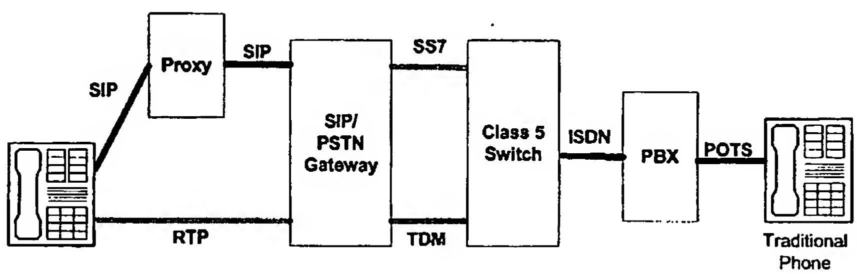
The only IPv6 specific standard for SIP is an updated DHCP option to configure the SIP outbound proxy <RFC 3319>. This is required because DHCP has changed slightly between IPv4 and IPv6.

6 SIP and the PSTN

Telephony is the most developed SIP application, and the PSTN adds a range of specific requirements. These requirements fall into the categories of interoperability and regulatory, and the following sections describe the issues to be addressed in each area.

6.1 Interoperability

Full PSTN interoperability implies that a SIP phone, operating through a SIP to PSTN gateway, is a fully functional replacement to a traditional phone. In other words, a subscriber can access all existing services with a SIP phone even when some of those services are provided by a third party, for example corporate voicemail. This level of interoperability does not prevent a SIP phone from providing new services that cannot be provided on a traditional phone.



SIP was designed for Internet telephony, and not designed to replicate the PSTN, and this means that it cannot readily handle all PSTN features. The following is a list of the some of the more important areas of work to use SIP in the PSTN.

6.1.1 Overlap signaling

Overlap signaling is required when it is not possible to determine whether a particular sequence of digits represents a valid phone number without attempting to place the call. This situation exists in various networks, including several European countries. In these networks, it is not possible to wait until the entire number has been entered before dialing, because the only way to detect this would be a pause in the entered digits. To allow a user to dial slowly, for example when referring to a telephone directory, a large delay between individual digits must be allowed (>10 seconds). If the exchange were to wait this length of time after the last digit to determine that the number was complete before placing the call, the delay in call-setup would be unacceptable. Therefore, when the user starts dialing, the telephone exchange waits for a minimum number of digits and a pause of a few seconds before using the digits collected to route the call onto the next hop. If the next hop has sufficient information, it continues to route the call onto its destination; otherwise it waits for further digits from the user before continuing.

This mechanism does not map easily onto SIP, because one subset of a number may not be routed the same way as another. As a result, when additional digits are received, a completely new SIP call must be made incorporating this new information, to enable the call to be routed independently. For all but one of the calls, the number will not represent a valid destination, and the call will fail with an "Address Incomplete" type of response, so only a single call remains.

It should be noted that a native SIP phone should not generate overlap dialing, because the user can be forced to enter the complete number before attempting to dial, as with mobile phones. However, when interoperating with traditional phones through SIP adaptor, or through a SIP gateway to the PSTN, overlap dialing cannot be avoided.

If an overlap-dialed call has to be routed from the SIP network into the PSTN, then all the calls placed as a result of overlap signaling must reach the same gateway and be correlated together. Otherwise, the gateway will not be able to generate overlap signaling in the PSTN, and will instead place multiple independent calls, which uses more resources.

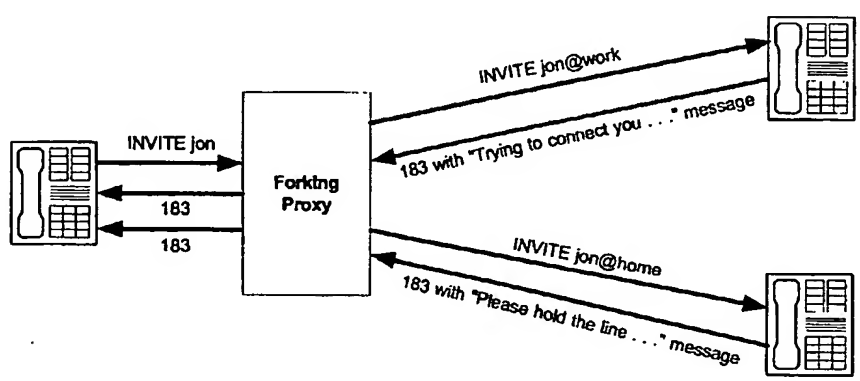
RFC 3578 describes this mechanism in more detail, although the standard is not yet widely implemented.

6.1.2 Early media

Early media describes media sessions that are started before the call setup completes. This is used in the PSTN for announcements during connection, such as "Trying to connect you ...", and to minimize the delay before the establishment of the media session once the call has connected.

Early media sessions require a mechanism to negotiate media channels before the call setup completes. This requires an ongoing exchange of messages between the caller and called party during call setup to agree these channels and any changes. The SIP protocol extension for reliable provisional responses (RFC 3262) provides such a mechanism, is the basis of early media in SIP, and is well supported.

Although early media works successfully, it does not work well with forking because a single forked call may establish multiple media streams. This is shown in the following diagram.



Here the call is forked and causes two phones to ring simultaneously. When both send back early media, what does the caller hear? Should one of the streams take priority over the other? The handling of this situation is under the control of the client application, but this complicates its design and there is no simple solution. For example, if the client application chooses one of the streams and then the other completes first, the caller may hear a very confused media stream.

This remains an area of ongoing concern, although it is not currently presenting a serious problem because forking is not widely used.

6.1.3 Application Control with a traditional phone keypad

The telephone keypad is often used to control telephony applications. These applications include

- information services, such as share prices and timetables
- calling-card services
- voicemail and unified messaging services.

Traditionally, key presses are encoded as DTMF and transmitted over the line with the voice. Using SIP, there are two methods to transport key presses: one is in the signaling channel, and the other is in the media channel. Both methods are needed to handle all of the above applications.

Calling-card applications need to monitor all key presses to control call setup, but once the call is put through, they are only interested in specific key sequences to regain control of the call to allow placement of a follow-on call; other key presses must be sent to the true destination of the call to control any application there. Monitoring the entire media stream by the calling-card application to detect these key sequences would be inefficient and would tie up media resources, so this type of application needs a mechanism to receive information on the key presses through the signaling channel.

Voicemail applications, on the other hand, may allow the user to record messages and announcements, controlled using key presses. In this situation, it is important that the keystrokes and media are synchronized in time, so that the recording starts and ends at the right time. This requires that the keystrokes be sent over the media channel, because this correlation cannot be provided over the signaling channel.

After much discussion and use of non-standard mechanisms, the following solutions have been proposed to handle each requirement.

- For the transport of key presses in the media stream, RFC 2833 provides suitable functionality, and this standard is now widely supported in SIP phones and application servers. It encodes the key presses into packets in the RTP media stream.

- There is still no final agreement on how to carry key presses in the signaling channel, but current proposals allow a device to ask the UA to send it each keystroke in a new SIP message. Further proposals include the ability to download a digit map to the client to allow it to monitor particular key sequences. The advantage is that this can decrease the number of messages required, but it also increases the complexity of the UA, especially if multiple devices want to monitor simultaneously.

Several existing SIP implementations use the INFO message to carry all key presses to devices in the signaling path. This method is inefficient because it sends all of the keystrokes through the signaling path, even when not required. It also raises scalability concerns, because there is no flow control mechanism to control the large number of messages that may be generated. As a result, the use of INFO messages is strongly discouraged.

There are also concerns over how multiple servers that are monitoring a single call should interact. For example, it is possible for several of them to place meaning onto the same key sequence; this is known as feature collision. One proposal to solve this uses Service Brokers, which act as a central point for other feature servers to interact with the call and resolve any conflicts.

6.2 Regulatory requirements

Telephony is heavily regulated because of its importance to the economy; it is fundamental to most businesses, provides access to the emergency services, and is monitored by the security services. To provide a full PSTN replacement service, the SIP network has to meet the same regulatory standards for features, quality and reliability.

Regulation of Internet telephony is already happening in many countries, although it is unclear how successful this process can be, given the ability to make phone calls over the Internet without any central point of control. The incumbent Telcos are also working to increase regulation of the Internet telephony service providers, in order to limit its growth and to raise the barriers to entry into the industry.

Compliance with these regulations also brings benefits in the form of government subsidies in many countries. There is therefore an incentive for Internet telephony service providers to comply with government telecommunications regulations whenever possible.

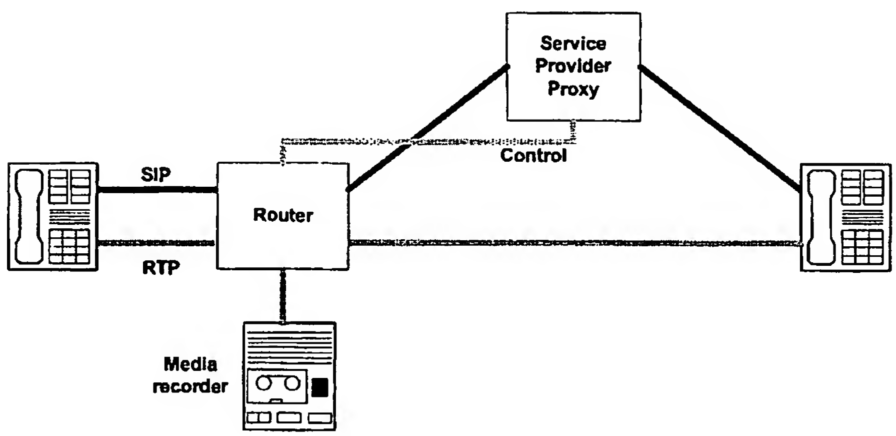
For a SIP-based telephone network to satisfy all its regulations, it will need to look a lot like the PSTN, with redundancy, media reservation, local feature servers and wire tapping capabilities. Reliability, scalability and QoS are more general requirements, and these were covered in Chapter 5. The following sections describe the other PSTN-specific requirements in more detail.

6.2.1 Wire-tapping

In most countries, the government is able to monitor selected telephone calls to or from individuals, without the knowledge of that individual. For traditional telephone companies, this is provided through the local exchange, which handles both the signaling and the media for every call.

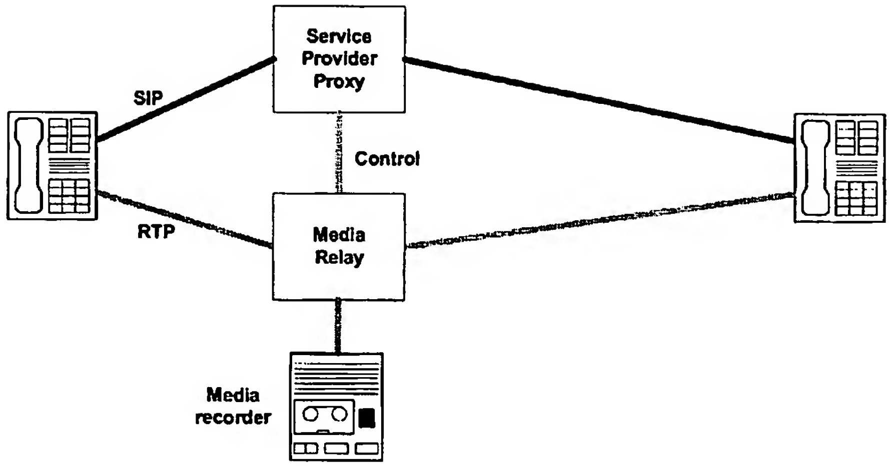
In the IP world of SIP, there may not be a telephone service provider, and there is no longer a simple central point at which to monitor the calls. However, assuming that a SIP telephone provider is being used, then their proxy may be used to monitor the signaling and to record information including the source, destination and duration of any calls.

Monitoring of the media is more complicated, as media is normally sent directly between user agents over a separate route. The only way to monitor such traffic is by packet sniffing at the router at the boundary of the customer's connection to the Internet, as shown below. This is a very processor-intensive process, and is further complicated if the customer has multiple links.



An alternative solution to direct only the monitored traffic through a media relay, where the call could be recorded, is also not possible, because one of the requirements is that it is not possible to detect that you are being monitored. The very act of redirecting the media identifies that the call may be being monitored.

It may also be possible to direct all traffic through a media relay, and some equipment manufacturers are using this solution, but this puts a heavy load onto equipment in the core of the network. In addition, there is no way to enforce this over the Internet without installing very restrictive firewalls to prevent direct media communication.



This issue remains unresolved, although the CALEA requirements in the US and similar proposals in other countries are addressing this issue. Current indications are that the regulations will impose the ability to monitor all traffic at the network edge, including telephony. However there is significant lobbying to limit the resulting intrusion of privacy and its enormous implementation costs.

6.2.2 Emergency calls

Due to their importance, calls to the emergency services are regulated separately from other calls. These regulations include the following.

Location determination

- The call should be handled by the local emergency service, so that the local police or ambulance service is always called. This requires knowledge of the location of the user, which is not available through SIP, because the IP address cannot always identify the location.
- Caller identification is required to allow the emergency service to know the location of the call, to allow them to dispatch help to the correct location, even when the caller cannot convey their location. This private information must also be withheld from other users.

Both of these can be provided by local configuration and the inclusion of caller location fields in emergency call requests. However, the use of local configuration risks the information being out of date. The IETF GEOPRIV working group is discussing the management of location information using DHCP, which would enable a device to determine its location from a central server. This potentially provides a long-term solution to this problem, but also places a requirement on service providers to manage this additional information.

Special handling of emergency calls

- Emergency calls should be given higher priority by the network. draft-ietf-sip-resource-priority-01 defines additional SIP headers that categorize the priority of a request. These new headers do not affect the operation of any IP routers in the network, but may be used by the SIP-enabled devices to prioritize their processing of the messages and to allocate higher priority to the IP packets to enable faster routing through the network.
- Calls to the emergency services are allowed even if the user is not an authenticated user of the network, for example with roaming mobile phones. There is no standardized method to allow this, and in particular it is not clear how the phone would know where to call without being authenticated and receiving local configuration information.

Work on all these issues is ongoing in the standards bodies, together with close liaison with the regulators to ensure that any solution is acceptable to them.

7 Enhanced applications for SIP

This chapter discusses some of the areas for which SIP is being developed, which will enhance the range of facilities that are currently available.

7.1 Mobile (3G)

SIP was mandated for call signaling for revision 5 of the 3GPP proposals for mobile networks. In revision 6, SIP's use is being extended to include presence. Revision 6 is scheduled to be frozen in March 2004.

The mobile environment presents a very different environment from a traditional SIP network, and this has required several extensions to the protocol. Its main characteristics and their effects include the following.

- Bandwidth is expensive in any radio-based environment. SIP is a text-based protocol that was designed for high-bandwidth environments, and can be compressed to significantly reduce the bandwidth required. SigComp <RFC 3320> provides a generic compression framework that is suitable for SIP. It is optimized for a particular protocol through the use of a standard dictionary of commonly used terms within that protocol. The standard dictionary for SIP and SDP is defined in RFC 3485.

- IPv6 has been mandated by 3GPP for use throughout the network. The use of SIP with IPv6 was covered earlier, and presents no problems.

- Mobile users move between radio cells, but as they move they maintain the same IP address. As a result, this movement is invisible to SIP, and the signaling is unaffected.

- Extended registration is required to allow mobile users to roam (use their phones with foreign network providers), while maintaining their relationship with their home provider so that they receive a single invoice, and to access their personal settings such as voicemail. This is achieved by routing communications through a local proxy (to impose local rules and access to local resources) and through a home proxy (to provide consistent global services and access private settings).

  Some minor SIP extensions have been defined that force messages to travel through several proxies, and to obtain the necessary configuration information from the different domains. These extensions include RFC 3327 (SIP Extension Header Field for Registering Non-Adjacent Contacts) and <draft-ietf-sip-scvrtdisco-04> (SIP Extension Header Field for Service Route Discovery During Registration).

With these extensions, SIP provides a flexible signaling framework for mobile telephony onto which new services, including presence and messaging, can be built.

7.2 Caller preferences

SIP has the ability to set up different types of communications session, including voice, video and instant messaging, and an individual user may have several SIP devices: for example at home, at the office and for mobile use.

When a call is received, the called party may, using pre-defined rules in a proxy or through an interactive choice, direct the call to any specific device. This choice may, for example, depend on the time of day, the identity of the caller, or the type of media requested. However, the caller may also have a preference over the device that is used to answer the call. For example, the caller may only want to talk if the called party is available at work, and does not want to be put through to voicemail.

Caller preferences allow the caller to request that the call only completes if certain conditions are met. Proxies and the recipient then use this information to decide how to route the call. The final destination of the call will therefore depend on both the caller's preferences and the called party's policy for handling incoming calls.

The success of this functionality relies on standard definitions for the types of device that are available to answer the call, and the willingness of the user to provide this information to a third party. <draft-ietf-sip-callee-caps-00> defines a way to describe the capabilities of a SIP device, and <draft-ietf-sip-callerprefs-09> defines how a caller can request to connect only to devices meeting selected criteria. These drafts, which are now getting close to standardization, provide the basis for this powerful feature.

7.3 Third party Call control

Third party call control refers to the ability for a device that is not one of the ends of the SIP signaling to affect a SIP dialog. It is required to provide PBX style services, such as call transfer and call screening, when there is no central PBX. There is no way to achieve this within the core SIP protocol, because the protocol is secured from end to end within a dialog, so several SIP extensions have been defined to enable this functionality.

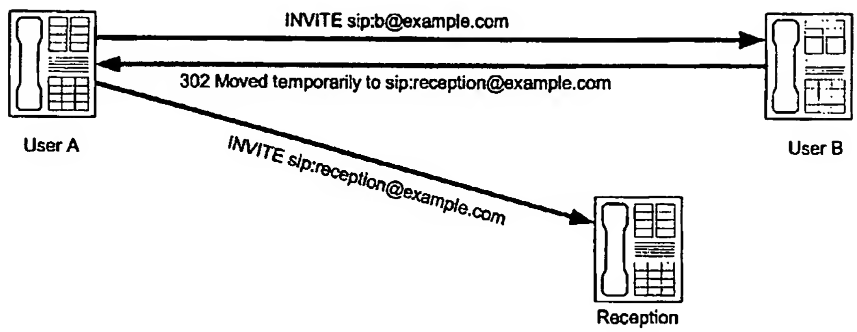
The following example shows a call screening service, which requires third party call control when there is no central PBX.

- A calls B, who has his calls forwarded to a receptionist.
- The receptionist checks with B whether he wants to take the call.
- The receptionist puts the caller through to B.

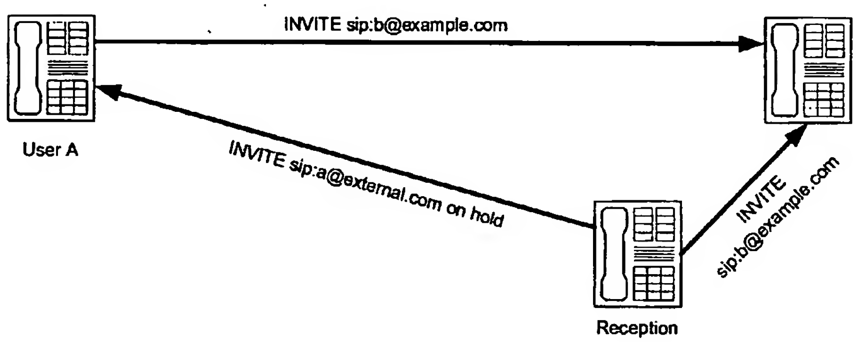
Third party call control is required for the receptionist to put the caller through to B, and to be removed from further involvement in the call.

Using SIP, this can work in the following way.

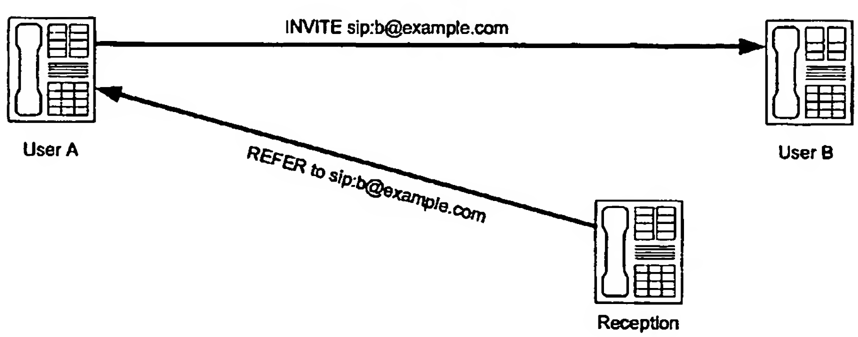
- B redirects all his calls to the receptionist using either his phone or a proxy, so that the initial call is established with the receptionist.



- After answering the call from A, the receptionist puts it on hold and calls B.



- The final stage requires the receptionist to set up a call between A and B to replace the two existing calls and to take the receptionist out of the loop.



The SIP REFER method (RFC 3515) allows a third party to request a SIP device to perform a defined action. In the call-screening example, REFER is used by the receptionist to cause A to call B directly.

There are several issues with this mechanism, in particular in relation to security. For example, if a person transfers their caller to a premium rate number, who pays for this call? Also, how is the second call put straight through, whereas the first call is diverted to the receptionist? Furthermore, it must not be possible for A to reuse any of this information in order to make a call directly to B at a later time and bypass his call forwarding.

REFER incorporates a security mechanism using a token that is passed by the REFERer to the REFERee to enable the REFERee to validate the authority of the REFERer. This provides the security required above, but it also requires an existing trust relationship between the referrer and referee to interpret the token. Although the meaning of the token is dependent on the particular environment, the current lack of standardization will cause interoperability problems between different vendor solutions.

7.4 Conferencing

VoIP conferencing today primarily uses H.323 as the signaling protocol. H.323 is well established in the market and has been extended to include conference control features. The use of SIP in conferencing applications is an area of intense interest and standardized mechanisms are being defined to add conference control.

Conferences fall into the following two categories.

- Tightly-coupled conferences have a central point of control. This is the traditional conferencing system, where a single server controls the conference and the media mixing.
- Loosely-coupled conferences have no central point of control; the users communicate directly with each other, and the control and media mixing may be distributed through the network.

The distinction between these conference types, and the requirements that they have, are discussed in detail in draft-ietf-sipping-cc-framework-01.

The use of SIP for tightly-coupled conferencing is well advanced, because this can be achieved using only standard telephony function, although more advanced features are being planned. Loosely-coupled conferences present a much more difficult problem, because of the difficulty of maintaining consistent state across conference participants as participants enter and leave. The control of loosely-coupled conferences is still an area of academic study, so the rest of this section is devoted to tightly-coupled conferences.

Conferencing imposes a wide range of high and low-level requirements, including the following.

Session control

- Conversion of a two-party call into a conference with three or more participants
- Conversion of a conference back into a two-party call when the other participants leave
- Invitation to new participant (dial-out)
- Acceptance of a new participant (dial-in)

Conference floor control

- view information on the other conference participants
- control who may join and speak in the conference.

Application-level conference control

- prearrange conferences
- create conferences on demand

With a SIP conference server, the session control requirements are covered by standard telephony and third party call control mechanisms. For example, REFER can be used to redirect a call to the right conference bridge.

Conference floor control requires that the participants have additional information about the other participants and can control their behavior. This could be provided by a conference-aware SIP phone, which might, for example, present a list of all the participants, and allow the conference chair to choose the next speaker or disconnect a participant.

The SIP Events mechanism <RFC 3265> provides the ability for one party to request additional status from another. This mechanism can be used by a conference server to request the status of the participants, and also by the participants to request the status of the other participants from the server. The information that would be provided is not yet standardized, but the conference state package <draft-ietf-sipping-conference-package-00> defines what this might include.

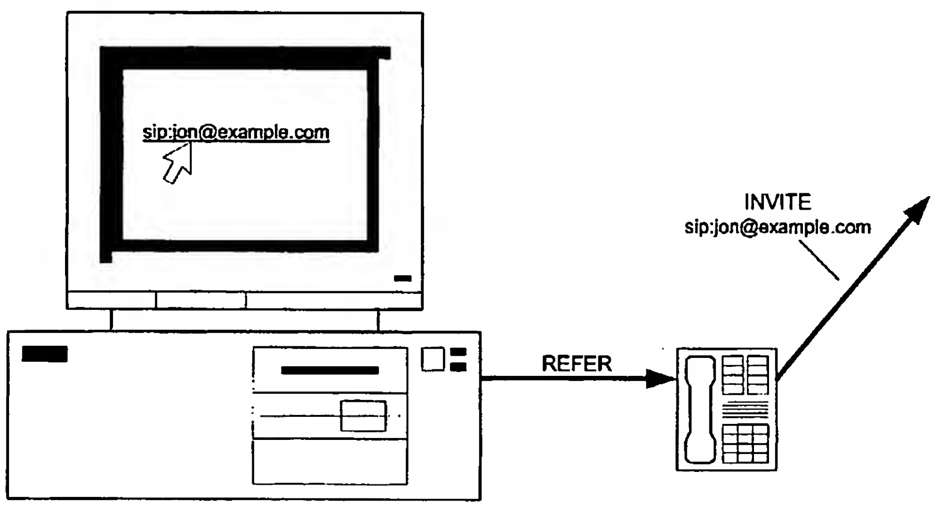
Conference control using SIP is still not well standardized, but work is continuing to bring consensus to this area. Solutions based on proprietary extensions are being developed, but until the standards mature, there will be limited interoperability of the higher-level features.

7.5 Click-to-call or click-to-dial

Click-to-call describes the ability for a hyperlink on a web page to initiate a telephone conversation to the referenced destination. This would be extremely useful in a web-based directory service or as a marketing tool. For example, it could be used to link directly from a company's website to a sales representative. However, in order for a click on a browser to initiate a phone call, the browser must be able to control the phone, and this functionality is not currently widely available.

Most people use a PC as their web browser, so the phone must either be a soft-phone on the same PC and integrated with the browser, or a hardware phone that is somehow under the PC's control. Soft-phones do not generally offer a great user experience, because PCs are not designed as telephones, and there is little integration between web browsers and proprietary phone systems to allow control of separate phones.

This integration of web and telephony was one of the early promises of SIP, but this is not yet widely used. A pure SIP solution to this problem requires a click in a browser to issue a REFER request to a designated phone to cause it to make the call. This is equivalent to the third party call control scenario described earlier.



Now that third party call control using SIP is being standardized, and suitable security enhancements are being defined to ensure that the system is secure, standardized browser extensions are possible to provide this functionality with any SIP phone.

The prevalence of this integration will increase rapidly as SIP replaces proprietary protocols in enterprise telephony systems, and as standard browser add-ins become available to control enterprise phones directly, using SIP, and indirectly through control of the PBX.

7.6 ENUM

ENUM aims to leverage the familiarity of existing telephone numbers on to Internet addresses. It defines a unique mapping between international phone numbers and host names in a way that enables DNS to be used to resolve the host name to an IP address, and the responsibility for maintenance of the DNS records to be delegated to the relevant country and regional authorities. The mapping is defined in RFC 2916, and, for example, +44 20 8366 1177 maps to 7.7.1.1.6.6.3.8.0.2.4.4.e164.arpa.

For SIP, ENUM provides a standard mapping between traditional phone numbers and Internet addresses, which could simplify the creation of an integrated PSTN and IP telephony system. However, there is currently very limited adoption of the standard and it is not gaining rapid traction. It would be straightforward to provide a default service provider as a gateway from the Internet into the PSTN, but it is not clear how this would be configured if multiple service providers are providing equivalent gateways.

draft-ietf-sipping-e164-04 describes the details of how to use ENUM to map between telephone numbers and SIP uris.

8 The future

Over the past 5 years, SIP has evolved from a flexible but limited protocol suitable for use in NAT-less IP networks, to a protocol in use across the Internet and at the core of the next generation of commercial telephony networks with their hybrid IP/TDM networks. Much work has been done to enhance SIP to support the QoS and other regulatory requirements, and it appears that most are now close to resolution.

With large-scale deployments such as Vonage and Yahoo!BB, and SIP phones now being mass-produced and available for under $100, the residential and SOHO markets are beginning to take off. At the same time, the increasing availability of SIP-enabled PBX solutions is driving enterprise adoption, and SIP deployments by the major carriers to replace the PSTN will start once all the regulatory issues are resolved. Every indication is that this combination will continue an exponential growth in SIP usage over the coming years.

The potential demand for VoIP is huge, but it is worth remembering that its users care about the services offered and the cost, rather than the underlying technology. Now that SIP equipment is becoming easy to install and use, broadband Internet providers can provide a basic telephony service at a very low cost, and increasingly they will offer such a service. Countering this, there will be increased charging for broadband connections based on bandwidth use, due to the spread of bandwidth-hungry applications, but this is unlikely to be at a level to impose a significant cost on audio services.

As margins are squeezed due to this increased competition, the network will increasingly becomes a commodity, and additional services, such as higher quality of service (QoS), interconnection to the PSTN, unified messaging systems, and mobile coverage will be the products that can command a premium.

The main risks to this picture are that

- the standards diverge as a result of the competing demands of its different uses, and that SIP loses the simplicity, interoperability and flexibility on which it was based
- the regulators limit the use of SIP telephony, or incumbent telephony suppliers maintain their monopoly grip and limit competition in the network provision
- SIP is dropped for use in next generation networks because its advantages are overwhelmed by commercial and regulatory requirements.

However, SIP has the opportunity to provide a flexible framework for true telephony interoperability between fixed, wireless, free and commercial services, and to provide seamless enhanced services across multiple networks.

Many powerful organizations are backing the use of SIP. Not all of them will be winners as a result of its success. Which ones are depends crucially on how the protocol develops and is deployed. If the protocol remains open and interoperable, then the user will benefit from increased competition and enhanced services. However, if the protocol becomes non-interoperable islands, then this promise will be delayed, although it seems unlikely that this progress will be stopped completely.

9 Further information

9.1 Web-sites

SIP working group	
Official site	http://www.ietf.org/html.charters/sip-charter.html
Supplemental site	www.softarmor.com/sipwg
SIPPING working group	
Official site	http://www.ietf.org/html.charters/sipping-charter.html
Supplemental site	www.softarmor.com/sipping
SIMPLE working group	
Official site	http://www.ietf.org/html.charters/simple-charter.html
Supplemental site	www.softarmor.com/simple
Others	
SIP Centre	www.sipcenter.com
SIP Forum	www.sipforum.org
Henning's SIP pages	www.cs.columbia.edu/sip
PacketCable	www.packetcable.com
Multiservice Switching Forum (MSF)	www.msforum.org
International Packet Communications Consortium (IPCC)	www.packetcomm.org

9.2 IETF RFCs and drafts

9.2.1 Application Control with traditional keypad

RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

9.2.2 Early media

RFC 3311	SIP UPDATE message
RFC 3262	Reliability of Provisional Responses
draft-camarillo-sipping-early-media-02.txt	Early Media and Ringing Tone Generation in SIP

9.2.3 Overlap dialing

RFC 3578	Mapping of Integrated Services Digital Network (ISDN) User Part (ISUP) Overlap Signalling to SIP

9.2.4 3G Mobile

RFC 3320	Signaling Compression (SigComp)
RFC 3327	SIP Extension for Registering Non-Adjacent Contacts
RFC 3485	The SIP and SDP Static Dictionary for Signaling Compression (SigComp)
draft-ietf-sipping-3gpp-r5-requirements-00.txt	3rd-Generation Partnership Project (3GPP) Release 5 requirements on SIP

9.2.5 AAA and security

draft-ietf-sip-authid-body-02	SIP Authenticated Identity Body (AIB) Format
draft-ietf-sip-identity-01	Enhancements for Authenticated Identity Management in SIP
draft-ietf-sip-smime-aes-01	S/MIME AES Requirement for SIP
draft-ietf-sipping-aaa-req-03.txt	Authentication, Authorization and Accounting Requirements for SIP
draft-mahy-sipping-smime-vs-digest-01.txt	Discussion of suitability: S/MIME instead of Digest Authentication in SIP
draft-jennings-sipping-certs-01	Certificate Discover for SIP

9.2.6 Caller Preferences

draft-ietf-sip-callerprefs-09	Caller Preferences for SIP
draft-ietf-sip-callee-caps-00	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)

9.2.7 Conferencing

draft-ietf-sipping-3pcc-04	Best Current Practices for Third Party Call Control in SIP
draft-rosenberg-sipping-conferencing-framework-01.txt	A Framework for Conferencing with SIP

9.2.8 NAT and firewall traversal

RFC 3489	STUN - Simple Traversal of UDP Through NATs
RFC 3581	An extension to SIP for Symmetric Response Routing
draft-ietf-mmusic-sdp4nat-05	RTCP attribute in SDP
draft-ietf-mmusic-rtsp-nat-01	How to Enable Real-Time Streaming Protocol (RTSP) traverse Network Address Translators (NAT) and interact with Firewalls.
draft-rosenberg-midcom-turn-01	Traversal Using Relay NAT (TURN)
draft-rosenberg-sipping-ice-01	Interactive Connectivity Establishment (ICE): A Methodology for NAT Traversal for SIP

9.2.9 Device configuration

RFC 3361	DHCP Option for SIP
draft-ietf-sipping-config-framework-00	A Framework for SIP User Agent Configuration
draft-ietf-sip-mib-07	Management Information Base for Session Initiation Protocol (SIP)

9.2.10 Presence and Instant Messaging

RFC 3265	SIP Specific Event Notification
RFC 3428	Session Initiation Protocol Extension for Instant Messaging
draft-ietf-simple-message-sessions-01	Instant Message Sessions in SIMPLE
draft-ietf-simple-presence-10	A Presence Event Package for the Session Initiation Protocol (SIP)
draft-houri-simple-arch-01	SIP/SIMPLE Based Presence and IM Architecture

9.2.11 QoS

RFC 3312	Integration of Resource Management and SIP
RFC 3313	Private SIP Extensions for Media Authorization
draft-ietf-sip-resource-priority-01.txt	Communications Resource Priority for SIP

9.2.12 Other documents

MSF Technical Report MSF-TR-QoS-001-FINAL	Quality of Service for Next Generation Voice over IP Networks
PacketCable Specification PKT-SP-DQOS-I03_021116	PacketCable Dynamic Quality of Service Specification

10 About Data Connection Limited (DCL)

Data Connection Limited (DCL) is the leading independent developer and supplier of portable protocol software suites for VoIP (SIP, MGCP, Megaco), VPN (RFC 2547 MPLS/BGP, Martini, VPLS), IP Routing (OSPF, IS-IS, BGP, CSPF), MPLS (GMPLS, UNI, NNI), ATM (PNNI, SPVC, UNI) and SNA, and Conferencing, Messaging, and Directory solutions. Customers include Alcatel, Cabletron, Cisco, Fujitsu, Hewlett-Packard, Hitachi, IBM Corp., Microsoft, Mitel, NEC, Nortel, Siemens, SGI and Sun.

DCL is headquartered in London UK, with US offices in Reston, VA and Alameda, CA. It was founded in 1981 and is privately held. During each of the past 21 years its profits have exceeded 20% of revenue. Last year, sales exceeded $40 million, of which over 90% were outside the UK, mostly in the US. Even through the current severe downturn, Data Connection's financial position remains secure, as does its employee base: its 200+ software engineers have an average length of service of 8 years, with turnover of <3% annually.

DC-SIP provides a complete SIP User Agent and Proxy toolkit for building high-performance SIP devices. DC-SIP supports the latest RFCs, including RFC 3261 and many extensions, and is used by customers around the world to build scalable and robust SIP devices. DC-SIP is supplied pre-integrated with Windows, Solaris, Linux, VxWorks, OSE and LynxOS, and is readily ported to other environments.

All of the Data Connection protocol implementations are designed for scalability, distribution across multiple processors, and fault tolerance. We have extremely consistent development processes that result in on-time delivery of highly robust and efficient software. This is backed up by an exceptionally responsive and expert support service, staffed by engineers with direct experience in developing the protocol solutions.

DCL also supplies integrated solutions incorporating SIP and its other technologies in web-conferencing and unified messaging solutions, and as a complete class 5 replacement switch through its Metaswitch division.

Data Connection is a trademark of Data Connection Limited and Data Connection Corporation. All other trademarks and registered trademarks are the property of their respective owners.

. Integrating Voicemail Systems

A white paper describing the integration of
heterogeneous voicemail systems

January 2004

Michael James
Internet Application Group
Michael.James@dataconnection.com

Internet Applications Group
Data Connection Limited
100 Church Street
Enfield
EN2 6BQ
United Kingdom
http://www.dataconnection.com

DATA CONNECTION

Table of contents

1 Introduction

1.1 Background

A history of mergers and acquisitions in the telecommunications industry has left many large carriers with voice messaging networks and systems from multiple vendors and with differing generations of technology. Carriers are looking for ways to offer broader messaging capabilities to subscribers without losing the investment in these legacy voicemail systems – but these systems were rarely designed to operate in a heterogeneous environment. Their lack of interoperability means that it is often difficult to offer even basic inter-system messaging.

Integrating wireline and wireless voicemail systems presents a similar problem. As individual carriers increasingly play a role in both wireline and wireless arenas, it becomes important to present a coherent messaging interface in both spaces to present a consistent identity, and simplify the user experience.

Carriers need to find ways to reduce operating costs. It may not be viable to migrate all users to a single voice messaging system, but by integrating the current, disparate systems, the carrier can simplify the administration of the combined platforms, and this reduces the costs of administration.

1.2 About this document

This white paper sets out

- the requirements for integrating voicemail systems
- a solution that Data Connection has created (in partnership with a large US carrier) that meets these requirements.

The specific requirements of any particular voicemail integration project will differ according to the carrier's objectives and according to the subset of legacy equipment. The solution presented in this white paper cannot be a comprehensive design to fit all scenarios, and the development of any integration solution will always require close consultation with the individual carrier to ensure an appropriate system is deployed.

1.3 About Data Connection

Data Connection has an unparalleled level of experience in legacy voicemail integration. As well as working with large North American telecommunications companies on solutions for over 10 years, we are also a key software messaging and directory technology supplier to several of the primary voicemail equipment manufacturers.

Data Connection is the leading independent developer and supplier of conferencing and next-generation messaging platforms, including voicemail, email, and unified messaging solutions. The company is also the leader in portable protocol stacks such as IP Routing, MPLS, ATM, SIP, MGCP/Megaco, SCTP, and SNA. Customers include SBC, Verizon, Colt, Microsoft, IBM, Cisco, Fujitsu, Hewlett-Packard, Hitachi, Lucent, Nortel Networks, SGI, Siemens and Sun.

Data Connection was founded in 1981 and is privately held. It is headquartered in London UK, with US offices in Reston, VA, Alameda, CA and Dallas, TX. For the financial year to August 31, 2003, earnings were $12M on revenues of $39M, representing the company's 22nd straight year of strong profitability supplying telecoms technology to carrier and OEM customers.

1.4 Contact

For further information please contact:

John Palombo
VP Sales, Internet Applications Group
Data Connection Ltd (DCL)

12007 Sunrise Valley Drive
Reston, VA 20191

Tel: (703) 715-4914
Fax: (703) 648-1480
Email: jp@dataconnection.com

Graeme MacArthur
VP, Internet Applications Group
Data Connection Ltd (DCL)

100 Church Street
Enfield, UK EN2 6BQ

Tel: (+44) 20 8366 1177
Fax: (+44) 20 8363 1039
Email: gmca@dataconnection.com

Web: http://www.dataconnection.com

2 Requirements

2.1 Why integrate messaging systems?

Many carriers find themselves in the position of operating two (or more!) messaging platforms, and it may not be viable to migrate all users to a common platform.

In heterogeneous voice messaging networks, a carrier's subscribers are spread across equipment of different types, from different manufacturers, and with varying degrees of out-of-the-box interoperability. Integrating these heterogeneous messaging systems allows inter-system messaging - the ability of one voice messaging subscriber on platform 'A' to send a message to another subscriber on platform 'B'.

- This may be desirable as a new end-user feature in itself. For example, a carrier operating both wireless and wireline networks can introduce the ability to send messages between both platforms.
- A carrier may wish to introduce a next-generation platform to offer new services. By integrating with the legacy system, only a subset of subscribers (typically those who are paying for new features) needs to be migrated to the new system, without loss of function to existing subscribers.

Integrating messaging platforms can also benefit the carrier by providing a common administration platform, simplifying operations and therefore reducing the ongoing costs.

2.2 Overview of requirements

For inter-system messaging to be viable, the following features are required.

- A common transport for platform 'A' to communicate with platform 'B'.
- A way for subscribers on each platform to address messages so that they are routed across the common transport correctly.
- Either a common message format, or a mechanism to convert message formats while relaying messages between the two platforms.
- A common management platform to allow operators to manage the disparate systems from a common interface and to allow easy migration of configuration information between the systems.

In addition, an integrated voicemail system must conform to any regulatory requirements.

The remainder of this section discusses each of these items in more detail.

2.3 Common transport

Legacy voicemail equipment was designed to work with the public switched telephone network (PSTN). The common interfaces are PSTN interfaces such as PRI and SMDI connections. These interfaces remain the primary way that users interact with the voicemail platform, but they are not a convenient transport mechanism for server-to-server inter-system messaging between dissimilar platforms.

Fortunately, the vast majority of the voice-messaging equipment deployed today exposes some level of IP connectivity. IP offers the following benefits.

- Carriers typically have IP backbones that can link geographically dispersed voicemail platforms.
- IP allows the use of standard general-purpose servers to integrate the legacy platforms without the need to introduce further PSTN-VoIP gateways.
- IP offers open standards for store and forward messaging.

If IP-based connectivity is not available on one of the platforms in the heterogeneous network then it is sometimes possible to migrate those subscribers who are on that 'non-IP' platform to an IP-enabled platform with spare capacity.

2.4 Subscriber database integration

Each voicemail system will have its own subscriber database, with an associated provisioning and billing/reporting system. In a heterogeneous network, a carrier may have implemented a meta-provisioning layer that presents a common provisioning interface across all platforms. Even so, it is still usually true that the subscriber information is maintained in several segregated stores, each store associated with one platform, geographical location, or operational center.

To facilitate and control inter-system messaging in a heterogeneous environment, it is very useful to have a consolidated and unified store of all subscriber information. Typically, this is a centralized **LDAP** (Lightweight Database Access Protocol) directory service that provides a central point of provisioning and subscriber management. This directory service also ensures that when sending or receiving messages between platforms, appropriate steps are taken to

- route the message correctly in the messaging backbone
- address the message correctly for delivery on the target platform
- map the originator address correctly to allow message reply function
- perform suitable message body conversion if the message format is different between the two platforms
- apply any regulatory messaging restrictions.

2.5 Message format

2.5.1 Messaging standards

Voicemail systems that offer IP-based connectivity typically use one of the following open standards.

- **AMIS-D** – a definition for voice messaging using the X.400 messaging protocols. It has fallen out of fashion in a similar way to the X.400 protocol itself, but a few carriers still have AMIS-D systems in their voice messaging networks.

- **VPIM** – a definition for voice messaging using the SMTP/MIME messaging protocols. SMTP is the most prevalent system for e-mail, and VPIM is becoming the protocol of choice for inter-system voice messaging. Many voicemail equipment manufacturers offer VPIM interfaces today, or at least have one in development.

If a carrier's voice messaging network includes a mix of AMIS-D and VPIM equipment then an AMIS-D <-> VPIM gateway is required (which will include an X.400<->SMTP gateway).

Even in a network comprised completely of VPIM-capable equipment from different vendors, the differing interpretation of open standards often prevents directly connecting these systems and achieving seamless interoperability. This can be due to issues such as the disjoint subscriber databases, differing addressing schemes, or even different codec support for the encoding of voice body parts.

2.5.2 Address transformation

The method that a voice messaging system uses to address internal mailbox-to-mailbox messages is not always the same as the scheme used when the message is to leave the platform (even in homogeneous environments). Internally the platform will typically use a subscriber's phone number as the unique identifier, as this is what the originator will typically enter, or locate via a short-code, when composing a message (or it will be available in the header of a message to which they are replying).

Mailbox-to-mailbox messages that leave the platform over an IP interface will typically have an e-mail based addressing scheme (SMTP for VPIM systems, and X.400 for AMIS-D and some other legacy platforms). This addressing scheme is usually designed to facilitate server-to-server message relay in homogeneous environments and may not be a suitable or interoperable addressing scheme for messaging between different vendors' solutions. This is clearly true when going between AMIS-D and VPIM, but it is also true in many AMIS-D only or VPIM-only heterogeneous architectures.

The message gateway used to connect the legacy systems will typically be responsible for performing transformations on the incoming 'recipient' and 'originator' addresses to accommodate any incompatibilities in addressing schemes employed on the different platforms. The 'originator' address is transformed to allow the use of this address by the recipient for message reply operations.

2.5.3 Body part conversion

Just as the voice message can be addressed in different ways, the actual contents of the message can be encoded in varying ways by different systems. The key differences are as follows.

- Messaging standard (e.g. VPIM which uses MIME body parts, whereas AMIS-D uses P22 body parts).
- Body part encoding (e.g. a MIME VPIM attachment may be 'binary','base-64', or 'quoted-printable').
- Voice encoding, i.e. the codec used (e.g. G.711, G.726, 32k ADPCM, etc).

If different systems in the voice messaging network do not have a common format then the messaging gateway will have to be able to convert the message contents during message relay. This may require on-the-fly voice message transcoding, which (depending on the codecs involved) can be a high computational overhead.

2.6 Common management

In order to provide inter-system messaging, subscriber addressing information from all of the disparate messaging systems needs to be accessible from each. To achieve this, the subscriber information needs to be combined in a centralized database (or if this is not feasible, the separate databases need to be at least synchronized and accessible by all message systems

Similarly, billing systems may also need to be coordinated.

Operational costs can be reduced if all subscriber administration and billing can be handled through a single, combined system.

2.7 Regulatory requirements

In the United States, regulatory restrictions mean that certain carriers are not allowed to provide mailbox-to-mailbox voice messaging between Local Access Transport Areas (LATAs). It is therefore a legal requirement for some carriers that, if they are allowing subscribers to send inter-system messages, they determine the LATA location of originator and recipient, and prevent message relay when they are different.

In certain areas, a carrier may have been given long-distance (LD) relief, and may be allowed to offer inter-LATA messaging. It is also true that even if a carrier is prevented from providing public inter-LATA messaging, the carrier is allowed to operate as its own long-distance provider within the organization. The legacy voicemail integration solution should therefore offer the following features:

- Correct identification of originator and recipient LATA
- Blocking of inter-LATA messages where no LD relief exists, and where either recipient or originator is not a carrier employee.

3 Integration solution

This section provides an overview of a voicemail integration solution developed by Data Connection.

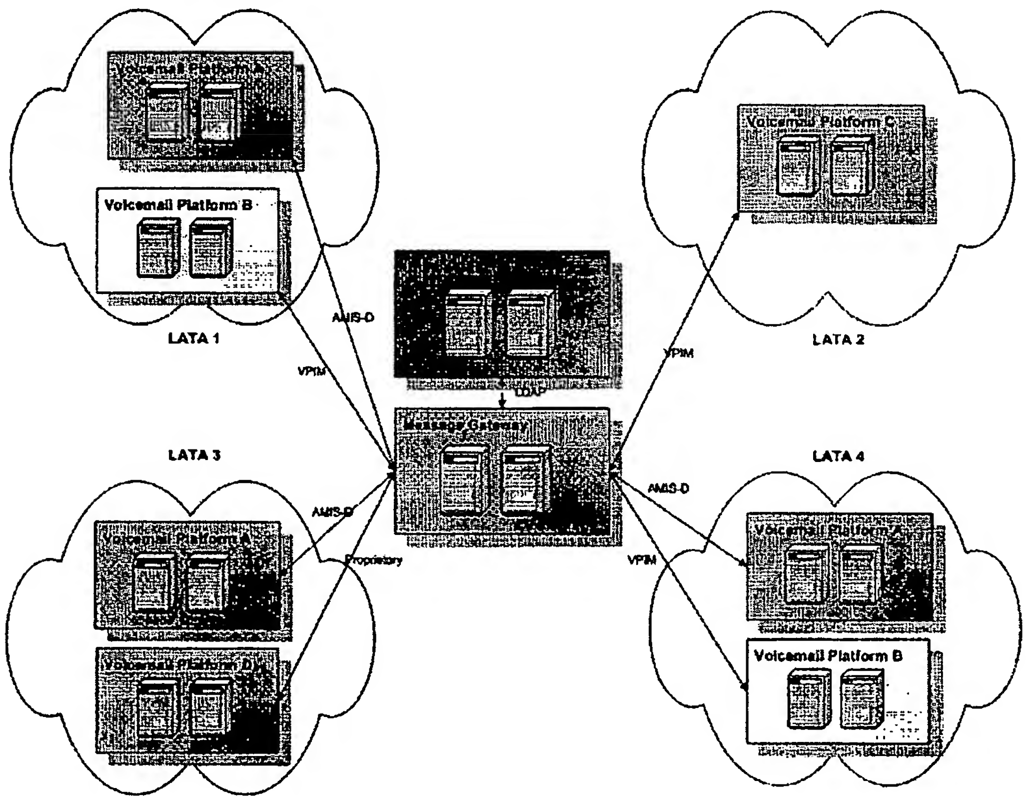


Figure 1. Integration of Legacy Voicemail Platforms

The two key components in the solution are:

- Unified Subscriber Directory
- Messaging Gateway

3.1 Unified subscriber directory

Data Connection's directory server DC-Directory is used as a central store for the collected subscriber information from all legacy voicemail systems. This can replace the subscriber store of the individual platforms, or they can co-exist using synchronization to ensure that the data is current in both locations. The method of synchronization is dependent on the interfaces that the legacy platform exposes. Initial population requires a bulk load of data into DC-Directory, and then future modifications are made by live updates, or scheduled incremental updates.

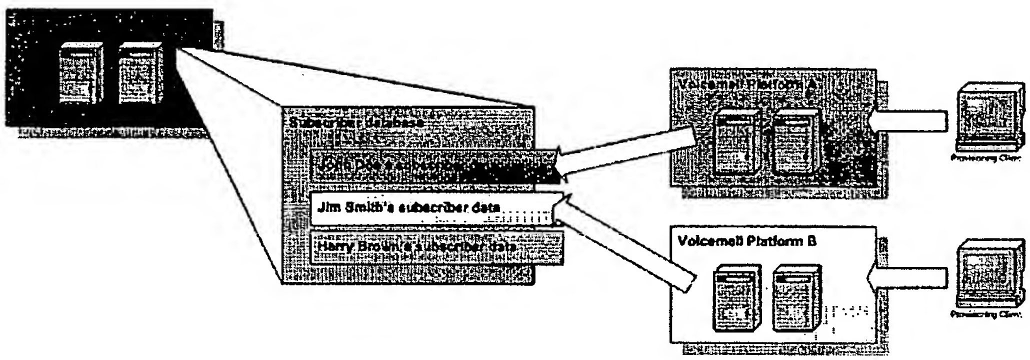


Figure 2. Bulk Load of Unified Directory

Bulk load requires a suitable mechanism for export of the subscriber data from the legacy voicemail platforms. This can be as simple as dumping the subscriber database to a fixed format file. This can then be pre-processed into a format suitable for import into the Unified Directory. The pre-processing step can be used to flag any data inconsistency and to normalize any variation in data formats from differing legacy systems.

One of the benefits of deploying a unified subscriber directory is that legacy platform provisioning may be centralized. By providing synchronization in the opposite direction, the unified subscriber directory may become the central point of provisioning and billing for all platforms.

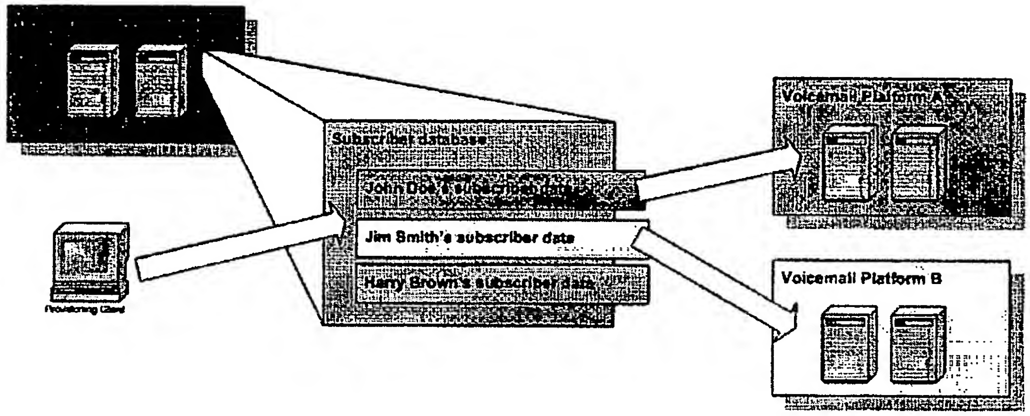


Figure 3. Centralized Provisioning though the Unified Directory

In some situations it may even be possible to remove the legacy platforms subscriber data store and have the legacy platform contact the Unified Directory for subscriber information. This reduces data duplication, but is depends on the legacy voicemail platform having enough flexibility to support an external directory – either by using LDAP calls directly, or by exposing a proprietary API or protocol that can be mapped to a set of LDAP calls.

If inter-LATA messaging is under regulatory restrictions then additional subscriber information must be available in the unified subscriber directory that is not normally stored per-subscriber in the legacy platforms. These additional fields can be derived or generated from other sources:

- LATA
- Carrier employee.

In situations where long-distance relief has been granted for some LATAs, the unified directory will also be the store for the data detailing which inter-LATA restrictions are in place.

3.2 Message gateway

Data Connection's integrated messaging server, MailNGen/Connect, provides the message gateway function that enables inter-system voice messaging.

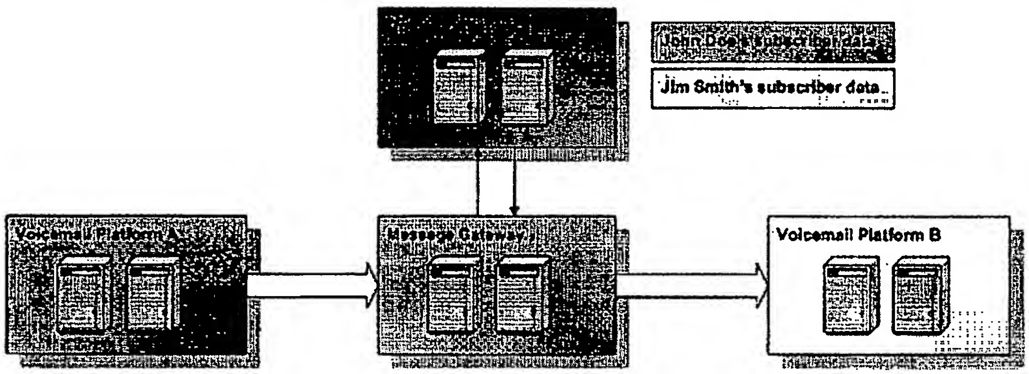


Figure 4. Message Gateway Operation

When John Doe sends a voice message addressed to subscriber Jim Smith, Platform A identifies Jim Smith as being a subscriber on a different platform, and so routes the message over IP to the message gateway. The message gateway receives the message and compares the LATA information of John Doe and Jim Smith to check that inter-system messaging is allowed.

Depending on the type of systems Platform A and B, the following steps may be performed:

- message type conversion (e.g. SMTP to X.400)
- originator and recipient address transformation, for correct message routing and reply function
- body part conversion and/or transcoding.

MailNGen/Connect can handle a range of message conversions, including:

- Voice messaging system: VPIM, AMIS-D, proprietary
- Messaging transport: SMTP, X.400
- Codec: G.711, G.726, 32kbps ADPCM, 16kbps RELP
- Encoding: base-64, binary, quoted-printable, ASN.1/binary.

3.3 Key features

The key features of the MailNGen/Connect solution are as follows.

- Connectivity and interoperability
    - Supporting the key internet standards (RFCs) and ITU standards (X.400) for voice and electronic messaging
    - Seamless gatewaying and migration capability between messaging platforms from a variety of vendors including Comverse, Unisys, DigitalSound (PulsePoint) and Octel legacy platforms and multi-media internet-based messaging systems
    - Directory-enabled, using LDAP for all configuration and subscriber information
    - Mature, extensively tested protocol engines (for both conformance and interoperability)
- Multi-platform support
    - Solaris
    - HP-UX
    - Linux
- Powerful messaging services
    - Scalable
    - High performance - gatewaying many messages per second
    - Reliable - continuous operation
    - Efficient - providing single-instance store for multi-recipient messages
- Operational management
    - System monitoring

      System alarms and operational statistics are generated. This information could be displayed by connecting the server to standard management workstations (such as HP OpenView).
    - Connection control and bandwidth management

      Automatic throttle-back protects against DoS attacks, and protection against open relay lessens the possibility of exploitation by spammers.

- Fault reporting

  A series of diagnostic logs is created to provide the information needed to accompany a fault report to ensure rapid resolution of a problem.

- System control

  Local management commands are provided to control the execution of the server.

- Service management

  A permanent log of the system's operation is provided for accounting and auditing, and to enable secure message tracking.

- Web management

  A Java-based web console allows both system monitoring and system control.

- Configuration

  - Via a simple Windows GUI application, which defines which remote messaging servers MailNGen/Connect connects to and the set of rules it uses to map email addresses and route messages.

- Support and consultancy

  - Product wholly developed by Data Connection, so our engineers are highly knowledgeable about the system
  - Comprehensive support and maintenance service
  - Professional consultancy services

4 Conclusion

Many carriers and service providers find themsclvcs in a position where they have a varicty of different and at best semi-compatible voicemail systems which they would like to upgrade both to reduce operating expenses and to offer new services, without losing their considerable investment in these legacy systems.

One solution to this problem is to enhance the legacy systems so that they can communicate directly and be managed through common protocols, such as VPIM and LDAP. However, in practicc, this can be difficult to achieve.

- Every legacy system has to be upgraded to work with every other system deployed in the network.
- Many of the common standards are open to interpretation, meaning that two implementations of the same standard may well not interoperate, which increases development and testing costs in the legacy systems.
- Vendors arc reluctant to invest significant development dollars in old equipment that is at or close to being end-of-life – both because of the sheer cost and the non-strategic nature of the investment.

An alternative solution is to use a single intermediary system that is dedicated to talking the right language to each legacy system. This can provide a cost effective and timely solution to the problem.

- It reduces the number of different interconnects that have to be agreed.
- Providing that the lcgacy systems provide some level of inter-messaging system communications, it is possible to fully integrate the legacy systems together without requiring any changes to them. The intermediary system can provide all of the required compensations for interoperability.
- The cost of implcmenting an intermediary system that has been specifically designed to interoperate with a wide variety of systems is likely to be a fraction of the cost of upgrading a legacy system.
- Unifying the management of the disparate systcms through the use of a master directory (for cxample, using LDAP) can also improve and simplify the integration with other back office systems such as those for billing and management. It also opens the way for adding other enhanced services such as subscriber self-care over a web-based interfacc.

Data Connection has a wealth of experience in integrating togcthcr legacy voicemail systems. Through a combination of providing both off-the-shelf products and development services Data Conncction can help Service Providers develop their voicemail capabilities in a timely and cost effective manner which preserves and maximizes the usc of their existing capital investments.

STRATEGIC COMPUTER TECHNOLOGY

DATA CONNECTION

Company
Products
Careers
Contact Us
Home
News
Search

MailNGen

Next generation messaging for Service Providers

MailNGen provides voicemail, email, webmail and fax messaging services, suitable for VoIP and traditional networks, with universal access from the phone and the desktop.

Its broad range of features and functionality allows Service Providers to offer value-added messaging services to consumers, businesses, and virtual ISPs.

MailNGen features include

- **unified mailbox** for voicemail, fax and email messages
- **universal access**: listen to emails over the phone, play voicemails over the web, forward faxes as email, etc.
- **VoIP support** to access the mailbox in next-generation networks
- **proven scalability** to millions of mailboxes on a single, centrally administered fault tolerant system, using our unique distributed architecture
- flexible, customizable web and

- Download the MailNGen brochure
- Read our White Paper on Integrating Voicemail Systems
- Request more information

Messaging
MailNGen
Voicemail
Email
Unified Messaging

Conferencing
MeetingServer
Architecture and integration
Case Study

Directory
Overview
Directories Explained
DC-Directory
DC-Metalink

Technology For OEMs
OEM Solutions

Resources
Press Releases
Support
Quality
Customers
Company

telephony UIs suitable for **re-branded and co-branded** deployments
- full multi-foldered IMAP-based **webmail** interface
- **integrated address book**
- a **rich administrative UI** including quota management capabilities
- web-based **self-care** screens to reduce administrative overhead
- **fully standards-compliant** (IMAP, POP, SMTP, VoIP, PSTN, HTTP, VPIM, VXML, ...).

MailNGen's rich feature set makes it suitable for deployment in a variety of messaging applications, from basic voicemail or email systems through to full unified messaging for millions of mailboxes.

Proven technology

Data Connection has been a leading supplier of messaging solutions since 1987, supplying componentry to OEMs - such as Microsoft (Exchange) and Lotus (ccMail) - and packaged solutions to Service Providers and large end-users - such as COLT Telecom, the US Department of Defense and Citigroup.

MailNGen is built upon proven Data Connection infrastructure components including our scalable, distributed LDAP directory.

email: info@dataconnection.com

STRATEGIC COMPUTER TECHNOLOGY

DATA CONNECTION

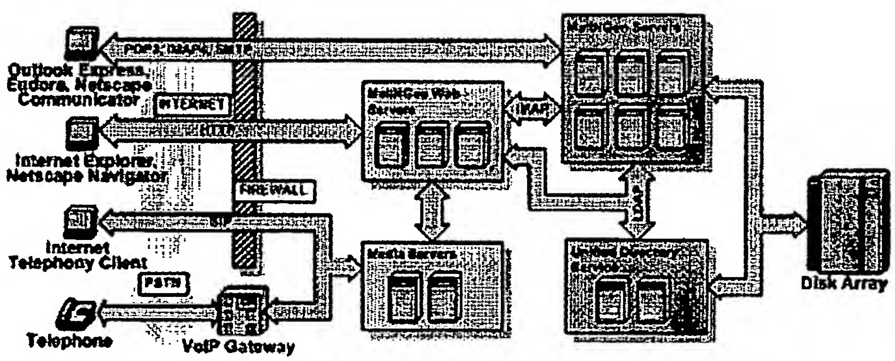
MailNGen

Unified Messaging

Just as many service providers are looking to converge their voice and data networks, users can see the advantage of unifying their mailboxes for voicemail, email, and fax messages.

Combining MailNGen's internet email and voicemail function gives everything a service provider needs to offer a rich Unified Messaging service, including

- universal access to all message types from telephone, web or email
- a single message store for all message types, as the solution has been architected to support Unified Messaging from the start
- support for VoIP access
- VoiceXML support, allowing rapid development of enhancements
- integration with third-party text-to-speech solutions, so that email can be accessed over the Telephony User Interface.



MailNGen's architecture scales for massive fault-tolerant deployments, supporting millions of registered subscriber mailboxes. The key to our scalability and fault tolerance is a high level of distribution, under which no single component is critical to the servicing of any mailbox - any component can fail without compromising access to any part of the service.

- Download the MailNGen brochure
- Request more information

STRATEGIC COMPUTER TECHNOLOGY

DATA CONNECTION

Company
Products
Careers
Contact Us
Home
News
Search

MeetingServer

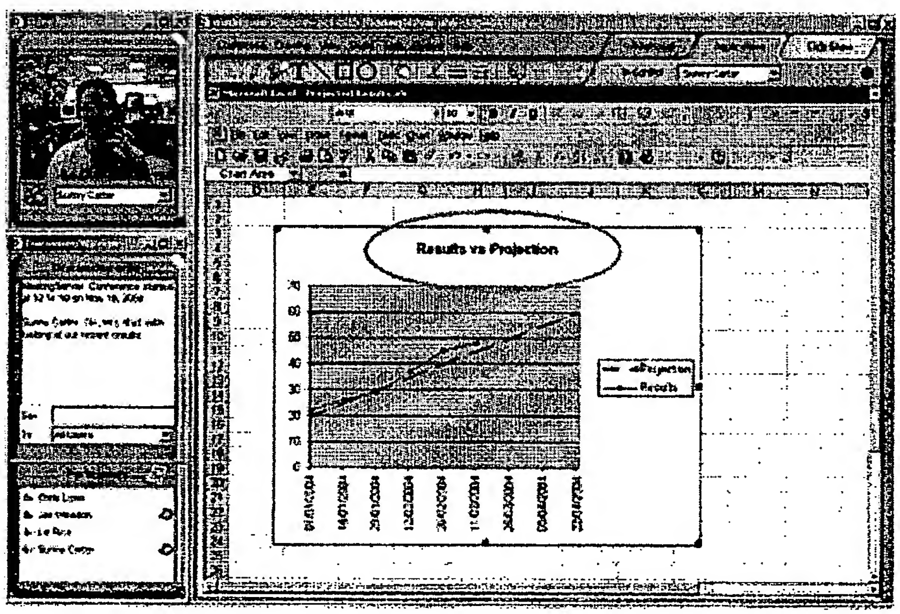
The award-winning web conferencing solution for Service Providers

MeetingServer is a carrier-grade, high-function, web conference server solution that allows Service Providers to deploy a robust, scalable, manageable web conferencing service to consumers, enterprises and virtual ISPs.

MeetingServer is also suitable for deployment directly within large enterprises that want to have the closer control - and lower costs - that only a powerful, flexible in-house web conferencing system can provide.

"Deployment of MeetingServer is likely to allow Service Providers to gain a better position in the conferencing market" - Jim Regan, Frost & Sullivan

Mi
Ma
Vo
En
Un
Re
Cc
Me
Fe
Arc
Ca
Ca
Re
Di
Ov
Dir
DC
DC
Te
Ap
OE
Go
Cc
Ab
Qu
Su
Re
Te
Cu
Pre
Wh
Pre
Da
co
aw



Web conferencing feature overview

- Easy-to-use, firewall-friendly **web conferencing** with high-performance application sharing, annotations, slide shows, whiteboard, voting, web video, and chat.

- Download the Product Information Sheet (243KB)
- Download a detailed MeetingServer Feature List (52KB)

- A **scalable** architecture supporting thousands of concurrent conferences and millions of registered users on a single server farm installation.
- Reservationless **web conference scheduling** with email invitation.
- Integrated with third-party audio bridges to provide an **integrated roster** of web and audio participants.
- The ability to **record both the audio and data portions of a conference** easily. Recordings can then be managed, annotated and published.
- A flexible, customizable UI suitable for **rebranding and co-branding** deployments.
- A range of **security features** including encrypted conferences.

- Request a demo of MeetingServer

Web conferencing technology

Data Connection has been the leading supplier of web conferencing technology to the industry's OEMs and Service Providers since 1991, with our software used by PictureTel, IBM, Sun Microsystems, SGI, Cisco and Latitude, in products such as SunForum and MeetingPlace.

This same technology is at the heart of Data Connection's packaged web conferencing solution, MeetingServer, which boasts the widest range of functionality and the highest performance of any web conference server.

For more information about Data Connection's web conferencing solutions, please contact meetingserver@dataconnection.com.

Home
email: info@dataconnection.com

STRATEGIC COMPUTER TECHNOLOGY

DATA CONNECTION

Company
Products
Careers
Contact Us
Home
News

Search

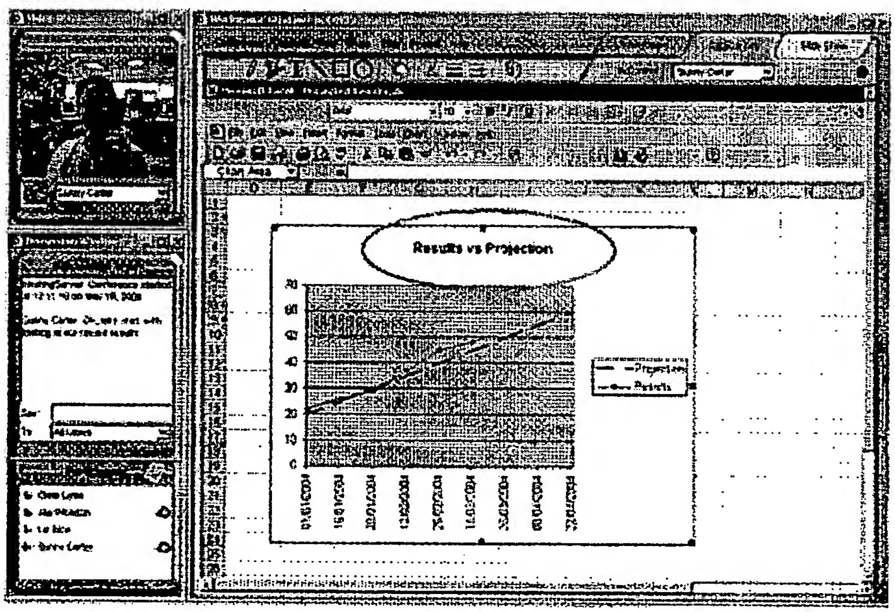
MeetingServer

The web conferencing solution for Service Providers

MeetingServer is a carrier-grade, high-function, conference server solution that allows Service Providers to deploy a robust, scalable, manageable web conferencing service to consumers, enterprises and virtual ISPs.

MeetingServer is also suitable for deployment directly within large enterprises that want to have the closer control - and lower costs - that only a powerful, flexible in-house system can provide.

"Deployment of MeetingServer is likely to allow Service Providers to gain a better position in the conferencing market"
- Jim Regan, Frost & Sullivan



Web conferencing feature overview

- Easy-to-use, firewall-friendly **web conferencing** with high-performance application sharing, annotations, slide shows, whiteboard,

- Download the Product Spec Sheet
A summary of MeetingServer's features
- Request a demo of MeetingServer

M
Ma
Vo
En
Un
C
Me
Ar
Ca
Di
Ov
Dir
DC
DC
Te
Ol
OE
R
Pr
Su
Qu
Cu
Co
Da
co
aw

voting, web video, and chat.
- A **scalable architecture** supporting thousands of concurrent conferences and millions of registered users on a single server farm installation.
- Reservationless **web conference scheduling** with email invitation.
- Integrated with third-party audio bridges to provide an **integrated roster** of web and audio participants.
- The ability to **record both the audio and data portions of a conference** easily. Recordings can then be managed, annotated and published.
- A flexible, customizable UI suitable for **rebranding and co-branding** deployments.
- A range of **security features** including encrypted conferences.

Web conferencing technology

Data Connection has been the leading supplier of web conferencing technology to the industry's OEMs and Service Providers since 1991, with our software used by PictureTel, IBM, Sun Microsystems, SGI, Cisco and Latitude, in products such as SunForum and MeetingPlace.

This same technology is at the heart of Data Connection's packaged web conferencing solution, MeetingServer, which boasts the widest range of functionality and the highest performance of any conference server.

For more information about Data Connection's conferencing solutions, please contact meetingserver@dataconnection.com.

Home
email: info@dataconnection.com

STRATEGIC COMPUTER TECHNOLOGY

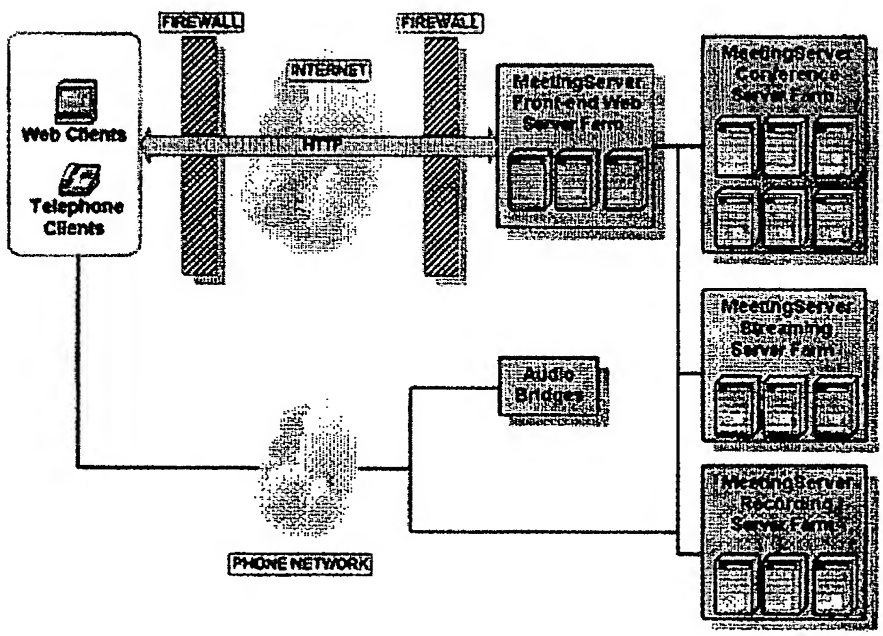
Company
Products
Careers
Contact Us
Home
News
Search

MeetingServer

Web conferencing architecture

MeetingServer's architecture is optimized for large-scale Service Provider deployments, supporting 10,000s of simultaneous web conferencing users (ports), but is also available for entry-level single server systems. A deployment can easily be enlarged simply by adding new servers, with no conference downtime.

The following diagram illustrates a distributed multi-server web conferencing deployment based on MeetingServer. The components shown in the diagram are described below.



- **Front-end web servers** provide the web-based user interface.
- **Conference servers** control active web conferences.
- **Recording servers** record both the audio and web parts of the conference as required.
- **Streaming servers** provide real-time streaming of recorded conferences.

In each server farm, multiple servers can be used for load balancing and fault tolerance. If you are setting a small conferencing deployment you may not need this, and can install all the conferencing features on a single server.

MeetingServer is integrated with **audio bridges** from several third-party vendors to offer a combined web and phone-based audio conferencing

Me
Ma
Voi
Em
Uni
Cc
Me
Arc
Ca
Di
Ov
Din
DC
DC
Te
OI
OE
Re
Pre
Su
Qu
Cu
Co
Dat
cor
aw

solution. Different audio bridge types can be used in a single MeetingServer deployment, presenting a unified conference bridge interface to users.

MeetingServer integration

When a Service Provider deploys a web conferencing service, it needs to ensure that the system meshes with other elements of the features it offers to its customers. MeetingServer is easily integrated with elements like billing, scheduling and authentication, and the interface look-and-feel can be customized for tailored, rebranded deployments. Data Connection can provide experienced Professional Services engineers to help.

Scheduling

MeetingServer uses a reservationless, "on demand" model for conference scheduling. As a result, no integration of scheduling databases is required.

Billing

MeetingServer writes billing information to a database. It is simple to configure MeetingServer to write this information into the appropriate fields of an existing, external billing database to combine web and audio conferencing details.

Authentication

For security purposes, some deployments require users to be authenticated before joining the conference. MeetingServer uses a simple HTTP request/response interface to authenticate clients with an external web server. No integration of user databases is required.

Branding

MeetingServer can be branded to project your own look-and-feel, and internationalized, by simply modifying text-based template files.

For more information about Data Connection's conferencing solutions, please contact meetingserver@dataconnection.com.

email: info@dataconnection.com